FBI PRIVACY THRESHOLD ANALYSIS (PTA)

(Equivalent to the DOJ Initial Privacy Assessment (IPA))

NAME OF SYSTEM / PROJECT: Remote access [redacted] b7E

BIKR FBI Unique Asset ID: N/A [Project still in early stages of development]

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: Division: Office of General Counsel Phone: [redacted] Room Number: PA-400	**FBI OGC/PCLU POC** Name: [redacted] b6 b7C Phone: Room Number: 7350

FBI DIVISION INTERMEDIATE APPROVALS [complete as necessary consonant with Division policy]

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: [insert division name]	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:
FBIHQ Division: Office of General Counsel	Signature: [signature] Date signed: 8/25/10 Name: Elaine Lammert Title: Chief of Staff, Office of General Counsel	Signature: Date signed: Name: Title:

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7338).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

Upon final FBI approval, FBI OGC/PCLU will distribute as follows:

1 - Signed original to file 190-HQ-C1321794 (fwd to JEH 1B204 via PA-520)

Copies (recipients please print/reproduce as needed for Program/Division file(s)):
1 - DOJ Office of Privacy and Civil Liberties (via e-mail to privacy@usdoj.gov)
(if classified, via hand delivery to 1331 Penn. Ave. NW, Suite 940, 20530)
2 - FBI OCIO / OIPP (JEH 9376, attn: [redacted])
1 - FBI SecD/AU (elec. copy: via e-mail to UC [redacted])
1 - RMD/RMAU (attn: [redacted])
2 - Program Division POC /Privacy Officer
2 - FBIHQ Division POC /Privacy Officer
1 - OGC\PCLU intranet
1 - PCLU UC
1 - PCLU Library
1 - PCLU Tickler

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS: [This section will be completed by the FBI PCLU/PCLO following PTA submission. The PTA drafter should skip to the next page and continue.]

_____ PIA is required by the E-Government Act.

_____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ____ Yes. ____ No (indicate reason):

_x___ PIA is not required for the following reason(s):
___ System does not collect, maintain, or disseminate PII.
___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
___ Information in the system relates to internal government operations.
___ System has been previously assessed under an evaluation similar to a PIA.
___ No significant privacy issues (or privacy issues are unchanged).
_x__ Other (describe): This PTA is intended to cover the infrastructure, which includes the physical laptop and wireless connectivity capabilities, and not the files or programs on the laptop that contain personally identifiable information (PII). The functions performed on the laptop will be similar if not identical to functions performed in the individual user's daily work activities, which are already covered under existing privacy documentation. Finally, although using a laptop with a wireless connection to process information outside the office poses additional security risks, those risks are mitigated through the use of encryption and other security measures, which are described in other documents.

Applicable SORN(s): N/A.

Notify FBI RMD/RIDS per MIOG 190.2.3? _x_ No ____ Yes--See sample EC on PCLU intranet website here: [redacted] b7E

SORN/SORN revision(s) required? _x__No ____Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? _x__No ____Yes (indicate forms affected):

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other: N/A.

David C. Larson, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 2/3/2016

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. **Provide a general description of the system or project that includes: name of the system/project, including associated acronyms; structure of the system/project, purpose; nature of the information in the system and how it will be used; who will have access to the information in the system and the manner of transmission to al users.** (This kind of information may be available in the System Security Plan, if available, or from a Concept of Operations document, and can be cut and pasted here.):

The FBI's Office of General Counsel (OGC) plans to access the FBI's unclassified network (UNET) remotely with FBI issued laptops [redacted] b7E This PTA is intended to cover the infrastructure, which includes the physical laptop and connectivity capabilities, and not the files or programs on the laptop that contain PII.

[redacted]

The functions performed on the laptop will be similar if not identical to functions performed in the individual user's daily work activities while located in the office. Although using a laptop with a wireless connection to process information outside the office poses additional security risks, such as the loss of information, which includes PII, those risks are mitigated through the use of encryption and other security measures, which are discussed in other documents.

2. Does the system/project collect, maintain, or disseminate any information about individuals in identifiable form, i.e., is information linked to or linkable to specific individuals (which is the definition of personally identifiable information (PII))?

__x__ NO **[If no, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval. Unless you are otherwise advised, no PIA is required.]**

In part, Section 208 of the E-Government Act requires a privacy impact assessment (PIA) before developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form. Section 208(d) defines "identifiable form" as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." Here, the information [redacted] is not in identifiable form. Thus, under Section 208 of the E-Government Act, a PIA is not required [redacted] However,

one could argue that the information transmitted [redacted] is in identifiable form once the transmission is complete, and therefore might trigger additional privacy documentation under Section 208. Thus, one should note that any application used to generate or receive the information transmitted should already be covered by applicable privacy documentation, which includes a discussion of how information is transmitted and received. b7E

Further, although files and programs on the laptops will obviously contain information in identifiable form, the individuals who utilize the laptops outside of the office will not be performing functions that are different from functions already performed in the office. The information contained within files and/or programs on the laptop is presumably covered under existing privacy documentation. Therefore, in accordance with M-03-22, this initiative does not require another PIA since the privacy issues were already assessed. Moreover, since this PTA only covers the laptop infrastructure and not the information in the files and/or programs on the laptop, a PIA is not required.

Similarly, 5 U.S.C. § 552a(e)(4) of the Privacy Act requires each agency that maintains a system of records to publish a system of records notice upon the establishment of or revisions to such system of records. 5 U.S.C. § 552a(a)(5) of the Privacy Act defines a system of records as a group of any records from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Here, the information [redacted] is not retrieved by an identifying particular. Thus, [redacted] constitute a system of records, and therefore the Privacy Act's system of records notice requirement is not triggered.

Further, although laptops may contain information about individuals, the users who utilize the laptops outside of the office will not be performing functions that are different from functions already performed in the office. Therefore, the information contained within files and/or programs on the laptops is presumably covered under existing systems of records notices. Moreover, since this PTA only covers the laptop infrastructure and not the information in the files and/or programs on the laptop, no additional Privacy Act requirements are triggered by the laptop infrastructure.

_____ YES [If yes, please continue.]

3. Does the system/project pertain only to government employees, contractors, or consultants?

_____ NO _____ YES

4. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ NO _____ YES

5. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project?

_____ NO _____ YES **If yes, check all that apply:**

_____ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. **Describe:**

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

_____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____ NO [If no, proceed to question 7.]

_____ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ YES [If yes, proceed to question 7.]

_____ NO

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

_____ YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

7. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

_____ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

_____ YES **If yes, provide date of last C&A certification/re-certification:**

_____ Don't Know.

8. Is this system/project the subject of an OMB-300 budget submission?

_____ NO _____ Don't know _____ YES **If yes, please provide the date and name or title of the OMB submission:**

9. Is this a national security system (as determined by the SecD)?

_____ NO _____ YES _____ Don't know

10. Status of System/ Project:

_____ This is a new system/ project in development. **[If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]**

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO [If no, proceed to next question (II.3).]

_____ YES If yes, indicate which of the following changes were involved **(mark all boxes that apply)**:

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other **[Provide brief explanation]:**

3. Does a PIA for this system/project already exist?

_____ NO _____ YES

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

____NO ____YES

[The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [redacted] b7E

BIKR FBI Unique Asset ID: 2011-003-01

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: Information Assurance Division: Security Phone: [redacted] Room Number: SPYB F-701	**FBI OGC/PCLU POC** Name: Phone: Room Number:

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Information Assurance	Signature: [redacted] Date signed: 6/1/2011 Name: [redacted] Title: Unit Chief	Signature: Date signed: 6/1/2011 Name: Robert Cox Title: Section Chief
FBIHQ Division: Security	Signature: Date signed: 6/1/2011 Name: My Harrison Title: Deputy Assistant Director	Signature: Date signed: 6/23/2011 Name: Michael Folmar Title: Assistant Director

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS: [This section will be completed by the FBI PCLU/PCLO following PTA submission. The PTA drafter should skip to the next page and continue.]

____ PIA is required by the E-Government Act.

____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ___ Yes. ___ No (indicate reason):

__X__ PIA is not required for the following reason(s):
- __X__ System does not collect, maintain, or disseminate PII. See Legal & Privacy Analysis
- ___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
- ___ Information in the system relates to internal government operations.
- ___ System has been previously assessed under an evaluation similar to a PIA.
- ___ No significant privacy issues (or privacy issues are unchanged).
- ___ Other (describe):

Applicable SORN(s): N/A

Notify FBI RMD/RIDS per MIOG 190.2.3? ___No ___Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? ___No ___Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? ___No ___Yes (indicate forms affected):

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

[redacted] Unit Chief Privacy and Civil Liberties Unit	Signature: Date Signed:	[redacted] 6/20/11
[redacted] Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 6/22/11	

b6
b7C

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

[redacted] is designed to provide users, primarily within the Security Division (SecD), an integrated view of the Certification and Accreditation (C&A) status of the FBI's information technology (IT) assets. [redacted] will provide management a more accurate and timely awareness of C&A activities; and will also allow for continuous monitoring, vulnerability scanning, and risk posture assessment of FBI IT systems. [redacted] will be the system repository for all documentation relating to the Certification and Accreditation process as defined by the Security Division. b7E

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

___X__ NO **[If no, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval. Unless you are otherwise advised, no PIA is required.]** Log-in information and passwords are the only data that are personally identifiable and the privacy impact is negligible.

_____ YES **[If yes, please continue.]**

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

_____ The information directly identifies specific individuals.

_____ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

_____ The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

___ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly. **[If you checked this item, STOP here after providing the requested description.]**

4. Does the system/project pertain only to government employees, contractors, or consultants?

_____ NO _____ YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ NO. **[If no, skip to question 7.]**

_____ YES. **[If yes, proceed to the next question.]**

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____ NO **[If no, proceed to question 7.]**

_____ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ NO

_____ YES **[If yes, proceed to question 7.]**

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

_____ YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

_____ NO _____ YES **If yes, check all that apply:**

_____ SSNs are important for other reasons. **Describe:**

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

_____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

8. Is the system operated by a contractor?

_____ No.

_____ Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

_____ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

_____ YES **If yes, please indicate the following, if known:**

Provide date of last C&A certification/re-certification:

Confidentiality: __Low __Moderate __High __Undefined

Integrity: __Low __Moderate __High __Undefined

Availability: __Low __Moderate __High __Undefined

_____ Not applicable – this system is only paper-based.

10. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

_____ NO

_____ YES **If yes, please describe the data mining function:**

11. Is this a national security system (as determined by the SecD)?

_____ NO _____ YES

12. Status of System/ Project:

_____ This is a new system/ project in development. **[If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]**

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO [If no, proceed to next question (II.3).]

_____ YES If yes, indicate which of the following changes were involved **(mark all changes that apply, and provide brief explanation for each marked change)**:

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other **[Provide brief explanation]:**

3. Does a PIA for this system/project already exist?

_____ NO _____ YES

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

____ NO ____YES

[The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

~~SECRET//NOFORN~~

Cover Unclassified when Detached from Document

(OGC/PCLU (Rev. 04/01/2011)

(U) FBI PRIVACY THRESHOLD ANALYSIS (PTA)

(U) NAME OF SYSTEM / PROJECT: [redacted] b7E

(U) BIKR FBI Unique Asset ID: NEN-0000079

Derived From: FBI NSISC-20090615 Classified By: F48M74K85 Reason: Declassify On: 20370516	SYSTEM/PROJECT POC Name: ITS [redacted] Program Office: Remote Operations Unit Division: Operational Technology Phone: [redacted] Room Number: 3A51-E	FBI OGC/PCLU POC Name: AGC: [redacted] Phone: [redacted] Room Number: 7350 JEH

b6
b7C

(U) FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:
FBIHQ Division: Operational Technology Division (OTD)	Signature: [redacted] Date signed: 7/16/12 Name: SSA [redacted] Title: Unit Chief, Remote Operations Unit	Signature: [redacted] Date signed: 07/17/2012 Name: SSA Rick Voss Title: Section Chief & Division Privacy Officer

b6
b7C

(U) After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350). (The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

~~SECRET//NOFORN~~

~~SECRET / NOFORN~~

(U) FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

_____ PIA is required by the E-Government Act.

_____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ____ Yes. ____ No (indicate reason):

__X__ PIA is not required for the following reason(s):
- _____ System does not collect, maintain, or disseminate PII.
- ____ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
- ____ Information in the system relates to internal government operations.
- ____ System has been previously assessed under an evaluation similar to a PIA.
- _____ No significant privacy issues (or privacy issues are unchanged).
- __X__ Other:

(U//FOUO) [redacted] (see description in PTA): [redacted] b7E

Applicable SORN(s): N/A

Notify FBI RMD/RIDS per MIOG 190.2.3? __X__ No ___Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? ___No ___Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? ___No ___Yes (indicate forms affected):
N/A

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

[redacted] Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed: 7/19/12	b6 b7C
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 7/20/12	

~~SECRET / NOFORN~~

(U) 1. INFORMATION ABOUT THE SYSTEM / PROJECT

(U) 1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

(S)

b1
b3
b7E

(U) 2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

__X__ NO [If no, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval. Unless you are otherwise advised, no PIA is required.]

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

(Equivalent to the DOJ Initial Privacy Assessment (IPA))

NAME OF SYSTEM / PROJECT: SharePoint MySites

BIKR FBI Unique Asset ID: TBD

Derived From: **Classified By:** **Reason:** **Declassify On:**	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: Division: Office of the Chief Knowledge Officer (OCKO) Phone: [redacted] Room Number: FBIHQ 1871	**FBI OGC/PCLU POC** Name: Phone: [redacted] Room Number: 7350

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS [complete as necessary consonant with Division policy]

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: [insert division name]	Signature: [signature] Date signed: 6/18/2010 Name: C. Clayton Gregg Title: Chief Knowledge Officer	Signature: Date signed: Name: Title:
FBIHQ Division: Office of the Chief Knowledge Officer (OCKO)	Signature: [signature] Date signed: 6/18/2010 Name: Barrett R. Nixon Title: Special Advisor to the Chief Knowledge Officer	Signature: Date signed: Name: Title:

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7338).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

Upon final FBI approval, FBI OGC/PCLU will distribute as follows:

1 - Signed original to file 190-HQ-C1321794 (fwd to JEH 1B204 via PA-520)

Copies (recipients please print/reproduce as needed for Program/Division file(s)):

1 - DOJ Office of Privacy and Civil Liberties (via e-mail to privacy@usdoj.gov)
(if classified, via hand delivery to 1331 Penn. Ave. NW, Suite 940, 20530)
2 - FBI OCIO / OIPP (JEH 9376, attn: [redacted])
1 - FBI SecD/AU (elec. copy: via e-mail to UC [redacted] & [redacted])
1 - RMD/RMAU (attn: [redacted])
2 - Program Division POC /Privacy Officer
2 - FBIHQ Division POC /Privacy Officer

1 - OGC\PCLU intrane
1 - PCLU UC
1 - PCLU Library
1 - PCLU Tickler

b6
b7C

_____ PIA is required by the E-Government Act.

_____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ___ Yes. ___ No (indicate reason):

_x___ PIA is not required for the following reason(s):
___ System does not collect, maintain, or disseminate PII.
___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
_x_ Information in the system relates to internal government operations.
Note: PCLU plans to separately analyze privacy for the benefit of our employees.
___ System has been previously assessed under an evaluation similar to a PIA.
___ No significant privacy issues (or privacy issues are unchanged).
___ Other (describe):

Applicable SORN(s): DOJ-014, Employee Directory Systems for the Department of Justice, 74 Fed. Reg. 57,194 (Nov. 4, 2009).

Notify FBI RMD/RIDS per MIOG 190.2.3? ___No _x__Yes--See sample EC on PCLU intranet website here: https://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? _x__No ___Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? ___No _x__Yes (indicate forms affected): The homepage for MySites will contain an (e)(3) notice drafted by the Project Manager in conjunction with guidance from PCLU.

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other: Although an information system that manages information related to internal government operations does not require a PIA, there are times where the information contained in the system is sensitive and thus raises privacy concerns that require an assessment beyond the PTA. Here, PCLU evaluated the nature of the information contained in MySites and determined that because the information is standard directory information used for business purposes, the system does not require an additional PIA for submission to DOJ's OPCL. However, PCLU plans to separately analyze privacy for the benefit of our employees.

David C. Larson, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 2/18/2010

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: name of the system/project, including associated acronyms; structure of the system/project, purpose; nature of the information in the system and how it will be used; who will have access to the information in the system and the manner of transmission to al users.

MySites will reside on FBINET, which is FBI's internal network, on the SharePoint platform. MySites is a type of employee directory system that contains employee name, work address, position title, grade level, work telephone number, work email address, assigned projects, communities of practice and interest, general professional skills, language skills, educational history, job related training, and other work related information. Some of the information in MySites will come from existing FBI systems. Any directory information not already maintained by the FBI in another system is entered into the system by the employee on a voluntary basis. All users of MySites may view directory information about other employees for the purpose of facilitating professional contacts in order to perform FBI duties and to benefit the FBI's business practices. Information is retrieved from MySites by employee name. An employee has the ability to verify and edit most of the employee's own information in the directory system for accuracy. Skills and educational information from the Bureau Personnel Management System (BPMS) will be in read only format and must be edited through BPMS. For directory information not already maintained by the FBI, employees will be provided with a Privacy Act notice, as required by 5 U.S.C. § 552a(e)(3), at the time of collection. FBI does not anticipate sharing information contained within MySites with individuals outside of the FBI. However, if FBI determines that sharing is necessary, FBI will share information in accordance with 5 U.S.C. § 552a(b) of the Privacy Act, which includes sharing in accordance with any routine uses, as published in DOJ-014, that are compatible with the purpose for which the information was collected.

2. Does the system/project collect, maintain, or disseminate any information about individuals in identifiable form, i.e., is information linked to or linkable to specific individuals (which is the definition of personally identifiable information (PII))?

_____ NO **[If no, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval. Unless you are otherwise advised, no PIA is required.]**

__x__ YES [If yes, please continue.]

3. Does the system/project pertain only to government employees, contractors, or consultants?

_____ NO ____x__ YES

4. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ NO _x_____ YES

5. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project?

___x__ NO _____ YES **If yes, check all that apply:**

_____ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. **Describe:**

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

_____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____ NO [If no, proceed to question 7.]

___x__ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ YES [If yes, proceed to question 7.]

___x__ NO

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

___x__ YES **Identify any forms, paper or electronic, used to request such information from the information subject:** The homepage for MySites will contain an (e)(3) notice drafted by the Project Manager in conjunction with guidance from PCLU.

7. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

__x___ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

C&A was performed on SharePoint 2007, which is similar to the version of SharePoint that the developers anticipate will serve as the platform for MySites. The security staff was notified of the SharePoint upgrade on March 3, 2010 and C&A is expected to be completed in late June 2010.

_____ YES **If yes, provide date of last C&A certification/re-certification:**

_____ Don't Know.

8. Is this system/project the subject of an OMB-300 budget submission?

___X__ NO _____ Don't know _____ YES **If yes, please provide the date and name or title of the OMB submission:**

9. Is this a national security system (as determined by the SecD)?

__X___ NO _____ YES _____ Don't know

10. Status of System/ Project:

___x__ This is a new system/ project in development. **[If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]**

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO [If no, proceed to next question (II.3).]

_____ YES If yes, indicate which of the following changes were involved **(mark all boxes that apply)**:

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other **(Provide brief explanation)**:

3. Does a PIA for this system/project already exist?

_____ NO _____ YES

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

___ NO ___ YES

[The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

OGC/PCLU (Rev. 04/01/2011)

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Enterprise SharePoint Services

BIKR FBI Unique Asset ID: Proj2012-018-01

	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
	Name: [redacted] Program Office: WSSU Division: ITSD Phone: [redacted] Room Number: GP-703	Name: [redacted] Phone: [redacted] Room Number: FTTTF

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Information Technology Services Division	Signature: [redacted] Date signed: 9/6/2013 Name: [redacted] Title: Unit Chief	Signature: [redacted] Date signed: 9/20/13 Name: [redacted] Title: Unit Chief
FBIHQ Division: Information Technology Services Division	Signature: [redacted] Date signed: 9/6/2013 Name: [redacted] Title: Unit Chief	Signature: [redacted] Date signed: 9/20/13 Name: [redacted] Title: Unit Chief

b6
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

_X_ PIA is required by the E-Government Act.

____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? _X_ Yes. ___ No

____ PIA is not required for the following reason(s):
___ System does not collect, maintain, or disseminate PII.
___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
___ Information in the system relates to internal government operations.
___ System has been previously assessed under an evaluation similar to a PIA.
___ No significant privacy issues (or privacy issues are unchanged).
___ Other

Applicable SORN(s): SharePoint is not, by default, organized to retrieve information by name or personal identifier. However, SharePoint is purposefully easy to customize in ways that may include allowing users to retrieve information by name or personal identifier. Customized as such, the following SORNs apply: JUSTICE/FBI-002 (Central Records System); JUSTICE/FBI-022 (FBI Data Warehouse System).

Notify FBI RMD/RIDS per MIOG 190.2.3? ___No _X_Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

PCLU recommends WSSU confer with RMD regarding SharePoint records retention and FOIA issues.

SORN/SORN revision(s) required? _X_No ___Yes:

Prepare/revise/add Privacy Act (e)(3) statements for related forms? _X_No ___Yes:

RECORDS: The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

[redacted] Acting Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed: 8/08/2013
Christine M. Costello, Acting Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 9/9/13

b6
b7C

UNCLASSIFIED

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

a) **Name of the system/project, including associated acronyms**

This PTA covers Enterprise SharePoint Services. The FBI is currently migrating from SharePoint 2007 to SharePoint 2010 and, in the near future, virtualizing SharePoint environments within the SECRET Enclave as described below.

b) **Structure of the system/project, including interconnections with other projects or systems**

The Enterprise SharePoint Services system is a Sharepoint 2007/2010 Web Platform that uses Microsoft SQL Server as its database system within the FBI SECRET Enclave (FBINET). The system functions by presenting dynamic web pages to the customer through the FBI Intranet web browser and providing storage for data entered using SharePoint user interfaces. The Enterprise Sharepoint Services System connects into (and shares information with) the following FBI Information Systems on the FBI SECRET Enclave: [redacted] b7E Bureau Personnel Management System (BPMS), Active Directory, and Automated Case System (ACS). These connections are made through the use of multiple hosted Web Services.

The Web Services Support Unit (WSSU) currently has five SharePoint environments: Operations Test and Evaluation Facility (OTEF) SharePoint 2007/2010; Pre-production/Usability SharePoint 2007/2010; SharePoint 2007/2010 production environment; SharePoint 2007/2010 Recovery Farms; and SharePoint 2007/2010 Continuity of Operations (COOP) environment.

The OTEF SharePoint 2007/2010 environment is currently virtualized, meaning all SharePoint web front end servers (with which users interact) and Structured Query Language (SQL) databases[1] are hosted on virtual machines.[2]

[1] An "SQL database" is the back end of the SharePoint servers. It contains all content from SharePoint Web sites.

[2] A virtual machine is a software (virtual) implementation of a computing environment in which an Operating System or program can be installed and run. It is a popular way of providing additional low-cost web hosting services instead of requiring additional physical servers.

The SharePoint 2007/2010 Pre-production/Usability Testing environment is used for user acceptance testing. Systems within this environment use unclassified data for testing purposes. This environment does not contain information about individuals.

The FBI Distributed Application Virtual Environment (DAVE) Team has set up virtual machines for SharePoint Recovery Farms and Pre-production/Usability testing environments. In the near future, WSSU and DAVE teams will move forward to virtualize the SharePoint Production and COOP environments. The Recovery Farms and Pre-production/Usability testing environments will have all web front ends and SQL databases virtualized to test and observe how SharePoint works in the virtualized environments. Once these virtualized environments are up and running successfully on virtual machines, WSSU will move forward with virtualizing the Production and COOP environments. The web front ends and SQL databases of the Production and COOP SharePoint environments will be virtualized. These environments will no longer require additional physical servers when additional environments or operating systems are needed in most cases, but will use software (virtual) to create additional implementations of computing environments. Virtualization will not change access to SharePoint sites or security mandates and functionality. Virtualization will also not alter the type of content, applications, connections to other systems, or controls in place to govern the information flow for the previously mentioned items. It will, however, increase the efficiency of the FBI's infrastructure.

c) **Purpose of the system/project**

The purpose of the Enterprise SharePoint Services application is to provide a computing environment, including information storage capability, on the secure FBI SECRET Enclave that is feature-rich, easy to use, and customizable. For example, SharePoint provides a simple method for teams physically or organizationally spread throughout the FBI (Field Office, Branch, Section, and Unit) to collaborate on document drafting. These collaboration sites are used to coordinate communications between offices, or across hundreds of miles, for various classified and unclassified FBI objectives. Custom applications, which run on SharePoint, have been written for the purpose of supporting custom reporting requirements. [redacted] b7E

d) **Nature of the information in the system/project and how it will be used**

The nature of the information in the SharePoint OTEF and SharePoint Pre-production/Usability Testing environments is limited to non-production data, with no personally identifiable information, used for testing purposes.

The nature of the information displayed using SharePoint is highly varied, from administrative applications for approved training to operational intelligence reports.

SharePoint allows Special Agents to collaborate on working documents—such as FD-302s (Interview Forms)—prior to final submission to Sentinel. SharePoint also allows multiple geographically distant field offices, squads, or units to collaborate on special projects where one or more Field Offices work together to gather all applicable information regarding a case. Users can use SharePoint as a document repository for their Word, Excel, PowerPoint, and Visio documents for collaboration and dissemination purposes. Users can also set up Really Simple Syndication (RSS) feeds on SharePoint lists (collections of information shared by users) that they have created so that they can be automatically notified of changes to the list. Numerous uses of SharePoint have the potential to generate official records, as examples:

1. Forms - Users enter content into forms, which are presented using SharePoint, such as the FD-540 (Travel Request Form), FD-71 (Complaint/Assessment Form), and FD-1026 (GETA Training Request Form). Depending on the business requirements, some forms are only filled out and printed, but not stored on SharePoint. Other forms, and information collected via the forms, are maintained on the SharePoint site that hosts the information collection.

2. Custom applications - Many custom applications have been developed for SharePoint which act as user-friendly interfaces designed for certain tasks of presentation and manipulation of data. Some of these applications have as a part of the workflow, the transfer of the records into an official recordkeeping system, while other systems are official recordkeeping systems and do not require the export of records.

3. Ad-hoc, team, and other sites – SharePoint sites of all varieties may or may not contain official FBI records. Site Owners and Content managers are responsible for the proper management of the official records.

For SharePoint sites that do not automatically forward information to recordkeeping systems, the Bureau has no technological method of automatically monitoring whether such information is properly maintained on or forwarded to appropriate recordkeeping systems, maintained in compliance with NARA retention schedules, or produced in response to applicable FOIA or Privacy Act requests. In the absence of such automated capabilities, the FBI takes the following steps: (1) Regarding existing information in SharePoint, all SharePoint 2010 sites (see answer to Section I, question 6) include a privacy protection warning banner, with a link to the FBI's privacy policy and reference to the electronic recordkeeping policy; (2) Regarding creation of new SharePoint sites, and prior to destruction of existing SharePoint sites, SharePoint site requesters and owners are required to acknowledge their responsibilities with regard to records on a form that the FBI Office of the General Counsel, Privacy and Civil Liberties Unit (PCLU) is helping to develop. Policy to support this process is being developed by the FBI Records Management Division (RMD) and PCLU, which will establish procedures and responsibilities for the creation and deletion of SharePoint sites, including review by RMD and the OGC E-Discovery Unit before destruction. Until a policy has been finalized, any SharePoint

site destruction/deletion requests must be sent in the form of Electronic Communication to the attention of RMD Unit Chief [redacted] and Unit Chief [redacted] and OGC Unit Chief [redacted] The EC must include the following information: b6 b7C

- SharePoint site name,
- Name of the site owner and if needed a separate point of contact,
- URL of the site,
- Purpose of the site,
- Last known date the site was used,
- A statement of what type of records and information were housed on the site, and
- Into which repository the records and other information were moved.

Upon receipt of this EC, RMD and OGC will review and provide notification of authority to delete/destroy to ITSD which will then proceed with destruction/deletion and provide affirmative notification to RMD and OGC upon completion.

c) **Who will have access to the information in the system/project**

Presence Sites:
Everyone with FBINET access can access the Intranet FBI home page, main sites for field offices, and other unrestricted headquarters sites, which are all presented using SharePoint.

Internal Teamsites:
Teamsites specific to each field office, or Headquarters branch, division, section, or unit are generally not open for read, contribute, or design access by users outside the entity. However, entities are delegated permission controls to allow additional access to persons outside the entity on an as-needed basis.

Ad hoc Teamsites:
Teamsites for specific project collaboration may span across various divisions or field offices, are generally of short term duration and are access limited to those who need to know and/or contribute to the information on the site.

Form Sites:
Each form site hosts an official electronic form template, along with user guides, frequently asked questions, and points of contact. All users have access to the sites and to fill forms. Not all sites store filled forms, but those sites that do restrict access to only selected staff in the office responsible for the form.

Environments:

Production: Access to the production environment is described in the above Presence, Internal, Ad hoc and Forms Sites paragraphs.

For the **SharePoint OTEF** environment, access is limited to development staff of systems and SharePoint Administrators and developers of WSSU.

For the **SharePoint Pre-production** environment, limited content managers, systems development staff, FBI project staff, and users/stakeholders of the systems have access to perform testing.

Recovery Farm environments are only accessed by the System Administration person who is making a recovery. The recovery environment only exists during a recovery exercise and then is deleted.

The **Continuity of Operations environment** is only accessible by the System Administration staff.

f) **The manner of transmission to all users**

Transmission of information using SharePoint in OTEF, Pre-production/Usability testing, Production, Recovery Farms and COOP environments is through either Internet Explorer or Mozilla Firefox on the Secret Enclave of FBINET only.

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

_____ NO

__X__ YES However, the SharePoint pre-production environment will not contain personally identifiable information.

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

__X__ The information directly identifies specific individuals.

__X__ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

__X__ The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

____ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly.

4. **Does the system/project pertain only to government employees, contractors, or consultants?**

__X__ NO _____ YES

5. **Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?**

_____ NO. [If no, skip to question 7.]

__X__ YES. [If yes, proceed to the next question.]

6. **Does the system/project collect any information directly from the person who is the subject of the information?**

_____ NO [If no, proceed to question 7.]

__X__ YES

a. **Does the system/project support criminal, CT, or FCI investigations or assessments?**

_____ NO

__X__ YES [If yes, proceed to question 7.]

b. **Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?**

_____ NO [The program will need to work with PCLU to develop/implement the necessary form(s).]

__X__ YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

SharePoint presents many forms in electronic versions, including FD-540 (Travel Request Form), and FD-1026 (GETA Training Request Form). These forms have (e)(3) notices. If new forms are developed and placed on SharePoint, the unit developing the form must comply with Section (e)(3) of the Privacy Act and should consult with PCLU for questions and further guidance. See FBI Privacy Policy Implementation Guide at 28-29.

SharePoint also hosts many applications with free text opportunities to enter personally identifiable information about others or about one's self. Accordingly, a banner located

on top of all SharePoint 2010 sites states: "WARNING: Information available through SharePoint may be subject to the Privacy Act of 1974. [more]" The "[more]" links to more detailed instructions, which state the following:

> Access to, and any contribution, sharing, or use of personally identifiable information available through SharePoint, including within documents uploaded to SharePoint pages, may be subject to the Privacy Act of 1974, 5 U.S.C. § 552a. The sharing of Personally Identifiable Information (PII) concerning United States Citizens and Lawful Permanent Residents is restricted to personnel with a "need to know." PII is any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. In addition, personnel utilizing SharePoint shall consider the sensitivity of any information prior to posting or accessing such information. Sensitive information, including PII, on SharePoint that appears to be unnecessary should be reported through the FBI Security Incident Reporting System. SharePoint Users and contributors are also required to adhere to all regulations and laws governing proper management of official FBI records, including but not limited to the Federal Records Act of 1950, 44 U.S.C. Chapters 31 and 33, and 36 C.F.R. Chapter XII. Required records management includes the records assessment of each SharePoint site and Electronic Recordkeeping Certification (ERKC), as required. *See*, ERKC policy at 66F-HQ-A1358157-POLL serial 157. For more information regarding FBI privacy policy and FBI personnel responsibilities regarding PII, please see the FBI Privacy Policy Implementation Guide, at http://home.fbinet.fbi/DO/OGC/LTB/PCLU/Privacy%20Libraries%20Library/Privacy%20Policy%20-%20Policy%20Implementation%20Guide.pdf.

WSSU has begun the process of migrating all SharePoint 2007 sites to SharePoint 2010 sites, which have the Warning banner and link to the more detailed instructions as referenced above. In an effort to disseminate the privacy warning prior to completion of that migration process—completion is anticipated May 2013—WSSU has prioritized the migration of the SharePoint help site and FBI Intranet home page to SharePoint 2010 so that users began to see the warning banners on those frequently visited sites beginning December 15, 2012.

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

_____ NO __X__ YES **If yes, check all that apply:**

__X__ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

FBI personnel using SharePoint to create case-related documents may include SSNs in addition to other information for identification purposes.

__X__ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. **Describe:**

__X__ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

Accesses to the sites that specifically request SSNs are highly restricted such that only personnel with a need to know the information have access. According to FBI policy, full SSNs should not be required from an individual unless that number is the only way to distinguish one person from another. Some SharePoint sites, and documents uploaded to SharePoint sites, allow free-text user entry of information such that a user could theoretically enter a SSN at their discretion. Users receive privacy training when they enter on duty and Information Security training with a privacy component each year during which they are reminded to keep secure personally identifiable information and only provide or make it accessible it to persons with a need to know.

_____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

8. **Is the system operated by a contractor?**

__X__ No.

____ Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. **Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?**

_____ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

__X__ YES **If yes, please indicate the following, if known:**

Provide date of last C&A certification/re-certification:

SharePoint falls under the C&A for FBINET (SECRET Enclave). The FBINET C&A was renewed March 14, 2012.

Confidentiality: __Low __Moderate _X_ High __Undefined

Integrity: __Low __Moderate _X_ High __Undefined

Availability: __Low __Moderate _X_ High __Undefined

_____ Not applicable – this system is only paper-based.

10. **Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?**

__X__ NO

_____ YES **If yes, please describe the data mining function:**

11. **Is this a national security system (as determined by the SecD)?**

__X__ NO _____ YES

12. **Status of System/ Project:**

_____ This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. **When was the system/project developed?** 2004

2. **Has the system/project undergone any significant changes since April 17, 2003?**

_____ NO. [If no, proceed to next question (II.3).]

__X__ **YES. If yes, indicate which of the following changes were involved (mark all changes that apply, and provide brief explanation for each marked change):**

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

__X__ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

Changes involve virtualization of the computing environment, which does not impact privacy or security concerns. The same security and access roles will be inherited into the newer, virtualized environments. Further, neither the changes in SharePoint 2007 nor SharePoint 2010 significantly impact privacy of information used in SharePoint compared to previous versions.

_____ Other **[Provide brief explanation]:**

3. Does a PIA for this system/project already exist?

__X__ NO _____ YES

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

___ NO ___ YES

~~SECRET//NOFORN~~

(OGC/PCLU (Rev. 06/08/2010)

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

(Equivalent to the DOJ Initial Privacy Assessment (IPA))

NAME OF SYSTEM / PROJECT: [redacted] b3 b7E

BIKR FBI Unique Asset ID: 0000060 and 0000247

Derived From: Multiple Sources Classified By: Reason: Declassify On: 20350707	SYSTEM/PROJECT POC Name: [redacted] Program Office: [redacted] Division: CTD Phone: [redacted] Room Number: 4512 b6 b7C b7E	FBI OGC/PCLU POC Name: [redacted] Phone: [redacted] Room Number: 7350 b6 b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: CTD [redacted] b7E	Signature: [redacted] Date signed: 10/19/2010 Name: [redacted] Title: Unit Chief b6 b7C	Signature: [redacted] Date signed: 10/19/2010 Name: [redacted] Title: CTD Privacy Officer b6 b7C
FBIHQ Division: CTD [redacted] b7E	Signature: [redacted] Date signed: 10/19/10 Name: Armando Fernandez Title: Section Chief	

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7338). (The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

Upon final FBI approval, FBI OGC/PCLU will distribute as follows:

1 - Signed original to file 190-HQ-C1321794 (fwd to JEH 1B204 via PA-520)

Copies (recipients please print/reproduce as needed for Program/Division file(s)):

1 - DOJ Office of Privacy and Civil Liberties (via e-mail to privacy@usdoj.gov)
(if classified, via hand delivery to 1331 Penn. Ave. NW, Suite 940, 20530)
2 - FBI OCIO / OIPP (JEH 9376, attn: [redacted])
1 - FBI SecD/AU (elec. copy: via e-mail to UC [redacted] & [redacted]) b6 b7C
1 - RMD/RMAU (attn: [redacted])
2 - Program Division POC /Privacy Officer
2 - FBIHQ Division POC /Privacy Officer
1 - OGC\PCLU intranet
1 - PCLU UC
1 - PCLU Library
1 - PCLU Tickler

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

____ PIA is required by the E-Government Act.

____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ___ Yes. ___ No (indicate reason):

__X__ PIA is not required for the following reason(s):
- ___ System does not collect, maintain, or disseminate PII.
- ___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
- ___ Information in the system relates to internal government operations.
- ___ System has been previously assessed under an evaluation similar to a PIA.
- __X__ No significant privacy issues (or **privacy issues are unchanged**).
- ___ Other (describe):

Applicable SORN(s): CRS, FBI-002

Notify FBI RMD/RIDS per MIOG 190.2.3? __X__ No ___ Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? __X__ No ___ Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? __X__ No ___ Yes (indicate forms affected):

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

Elizabeth Withnell, Acting Deputy General Counsel Acting FBI Privacy and Civil Liberties Officer	Signature: Elizabeth W. Withnell Date Signed: 10/9/10

~~SECRET//NOFORN~~

1. (U) INFORMATION ABOUT THE SYSTEM / PROJECT

1. (U) Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

(S)

b1
b3
b7E

(S)

b1
b3
b7E

(S) are available to FBI employees and detailees at FBI Headquarters, Field Offices, and Legats with appropriate clearances and a need-to-know that is certified in writing by their supervisor. access requires FBI employees and detailees hold Top Secret clearances and accounts on the FBI's Secret network.

b1
b3
b7E

(U) (U//NF) Information from the systems is put into an electronic communication (EC), which is an official FBI record and is maintained in the Bureau's automated case support system or is placed in another official FBI document, such as an intelligence assessment written by the Directorate of Intelligence. Dissemination is primarily through encrypted and secure electronic means, although information may also be disseminated in paper records.

(S)

b1
b3
b7E

2. (U) Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person)?

_____ (U) NO[**If no, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval. Unless you are otherwise advised, no PIA is required.**]

__X__ (U) YES [**If yes, please continue.**]

3. (U) Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

__X__ (U) The information directly identifies specific individuals.

__X__ (U) The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

__X__ (U) The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

(U) If you marked any of the above, proceed to Question 4.

____ (U) None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly. [**If you checked this item, STOP here after providing the requested description.**]

4. (U) Does the system/project pertain only to government employees, contractors, or consultants?

__X__ (U) NO _____ (U) YES

5. (U) Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ (U) NO. [**If no, skip to question 7.**]

__X__ (U) YES. [**If yes, proceed to the next question.**]

6. (U) Does the system/project collect any information directly from the person who is the subject of the information?

__X__ (U) NO [**If no, proceed to question 7.**]

_____ (U) YES

a. (U) Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ (U) NO

__X__ (U) YES **[If yes, proceed to question 7.]**

b. (U) Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ (U) NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

_____ (U) YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

7. (U) Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

__X__ (U) NO _____ (U) YES **If yes, check all that apply:**

(U) [redacted]

b3
b7E

_____ (U) SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ (U) SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ (U) SSNs are important for other reasons. **Describe:**

_____ (U) The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

__X__ (U) It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

(U) [redacted] b3 b7E

8. (U) Is the system operated by a contractor?

__X__ (U) No.
(U) However, contractors provide system administrative support to the Government.

____ (U) Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. (U) Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

_____ (U) NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

__X__ (U) YES **If yes, please indicate the following, if known:**

(U) **Provide date of last C&A certification/re-certification:** 8/9/2007, currently undergoing recertification

(U) **Confidentiality:** __Low __Moderate __X__High __Undefined

(U) **Integrity:** __Low __X__Moderate __High __Undefined

(U) **Availability:** __Low __X__Moderate __High __Undefined

_____ (U) Not applicable – this system is only paper-based.

10. Is this system/project the subject of an OMB-300 budget submission?

__X__ NO

_____ YES **If yes, please provide the date and name or title of the OMB submission:**

11. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53?

__X__ NO

_____ YES If yes, please describe the data mining function:

12. Is this a national security system (as determined by the SecD)?

_____ NO __X__ YES

13. Status of System/ Project:

_____ This is a new system/ project in development. **[If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]**

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?
   October, 2001

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO [If no, proceed to next question (II.3).]

__X__ YES If yes, indicate which of the following changes were involved **(mark all boxes that apply)**:

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

__X__ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

(U) There are quarterly updates from the originating agency, but none have significantly changed character or function of the system.

_____ Other **[Provide brief explanation]:**

3. Does a PIA for this system/project already exist?

_____ NO __X__ YES

If yes:

a. **Provide date/title of the PIA:** 4/15/2007, PIA for the [redacted] b3 b7E

b. Has the system/project undergone any significant changes since the PIA?

__X__ NO ____ YES

(U) (X/NF) [redacted] have not changed since the 2007 PIA. Other than the quarterly updates, there are only two changes: b3 b7E

(S) 1. (X/NF) The 2007 PIA indicated [redacted]

(S) [redacted] b1 b3 b7E

(S) [redacted] b1 b3 b7E

(OGC/PCLU Rev. 08/16/2010)

(OGC/PCLU (Rev. 08/16/2010)

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [redacted] b7E

BIKR FBI Unique Asset ID: _____

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: ITMD Division: D25-Intelligence Projects Phone: [redacted] Room Number: Crystal City, 4th Floor	**FBI OGC/PCLU POC** Name: [redacted] b6 b7C Phone: Room Number:

FBI DIVISION INTERMEDIATE APPROVALS [complete as necessary consonant with Division policy]

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: ITMD	Signature: Date signed: Name: Hien Bui Title: UC INTPU	Signature: [redacted] Date signed: 11/22/11 Name: [redacted] Title: ITS/ITB Privacy Officer
FBIHQ Division: ITB	Signature: [redacted] Date signed: 11/23/11 Name: [redacted] Title: UNIT CHIEF, INTPU	Signature: Date signed: Name: Title:

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS: [This section will be completed by the FBI PCLU/PCLO following PTA submission. The PTA drafter should skip to the next page and continue.]

_____ PIA is required by the E-Government Act.

_____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ___ Yes. ___ No (indicate reason):

__X__ PIA is not required for the following reason(s):
- ___ System does not collect, maintain, or disseminate PII.
- ___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
- ___ Information in the system relates to internal government operations.
- ___ System has been previously assessed under an evaluation similar to a PIA.
- ___ No significant privacy issues (or privacy issues are unchanged).
- __X__ Other (describe): Negligible privacy concerns as only log-in information is contained in the application.

Applicable SORN(s): To the extent records are retrieved by name or personal identifier, they are covered by DOJ-002, Computer Systems Activity and Access Records_____

Notify FBI RMD/RIDS per MIOG 190.2.3? __x_No ___Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? __x_No ___Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? __x_No ___Yes (indicate forms affected):

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

[redacted] Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed:
[redacted] Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: [redacted] Date Signed: 5/2/11

b6
b7C

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

[redacted] b7E

[redacted] is a commercial-off-the-shelf (COTS) software product (by [redacted] for project lifecycle management. It is used in: system requirements collection and management; mapping [redacted] tests to requirements; maintaining correction/defect lists; and displaying integrated dashboards showing project health, schedules, and status information. (A [redacted] assessment of [redacted] has been successfully completed.)

Only information necessary for project management will be retained by the [redacted] software tool. The only personally identifiable information (PII) that will be stored in the system consists of the login names and real names of [redacted] users (i.e., FBI employees and contractors). No operational or field data from any of the systems that [redacted] may support (including [redacted] systems) will be processed by or stored in [redacted]

The [redacted] software will reside on [redacted] servers and database will not reside within the security accreditation boundaries of [redacted] etc.; instead it will fall with the boundary of and be accredited under [redacted] The [redacted] software will rely on the [redacted] for login authentication.

[redacted] will have access to the data in the system. Any system/software administrators of the [redacted] software will be a small subset of the same group of persons. The system will be run on FBI-owned equipment within the FBI's [redacted] FBI contractors may assist in the installation and/or operations of the system.

Regular users will access [redacted] from the web browsers [redacted] After initial installation, all administrative functions will be performed through the same interface. During installation, administrators of [redacted] may also require access via [redacted]

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

_X_ NO **[If no, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval. Unless you are otherwise advised, no PIA is required.]** The only information that directly identifies a specific individual consists of information necessary to establish a login account, i.e., first and last name of account holder, and login pseudonym as copied from directly from the Bureau's central Active Directory.

____ YES **[If yes, please continue.]**

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

_____ The information directly identifies specific individuals.
_____ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

_____ The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

____ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly. **[If you checked this item, STOP here after providing the requested description.]**

4. Does the system/project pertain only to government employees, contractors, or consultants?

_____ NO _____ YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

____ NO. **[If no, skip to question 7.]**

_____ YES. **[If yes, proceed to the next question.]**

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____NO **[If no, proceed to question 7.]**

_____ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

____ NO

_____ YES **[If yes, proceed to question 7.]**

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

_____ YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

____ NO _____ YES **If yes, check all that apply**:

_____ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. **Describe:**

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

_____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

8. Is the system operated by a contractor?

_____No.

_____Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

___NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

_____ YES **If yes, please indicate the following, if known:**

Provide date of last C&A certification/re-certification:

Confidentiality: __Low __Moderate __High __Undefined

Integrity: __Low __Moderate __High __Undefined

Availability: __Low __Moderate __High __Undefined

_____ Not applicable – this system is only paper-based.

10. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?
___ NO

_____ YES **If yes, please describe the data mining function:**

11. Is this a national security system (as determined by the SecD)?

_____ NO _____ YES

12. Status of System/ Project:

_____ This is a new system/ project in development. **[If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]**

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO [If no, proceed to next question (II.3).]

_____ YES If yes, indicate which of the following changes were involved **(mark all changes that apply, and provide brief explanation for each marked change)**:

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other **[Provide brief explanation]:**

3. Does a PIA for this system/project already exist?

_____NO _____ YES

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

___NO ___YES

[The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

(OGC/PCLU (Rev. 04/01/2011)

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [redacted] b7E

BIKR FBI Unique Asset ID: N/A

Derived From: **Classified By:** **Reason:** **Declassify On:**	**SYSTEM/PROJECT POC** Name: IOA [redacted] Program Office: Division: St. Louis Field Office Phone: Room Number: [redacted]	**FBI OGC/PCLU POC** Name: AGC [redacted] b6 b7C Phone: [redacted] Room Number: 7350 JEH

FBI DIVISION INTERMEDIATE APPROVALS [complete as necessary consonant with Division policy]

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: St. Louis Field Office	Signature: [redacted] Date signed: 6/12/2012 Name: [redacted] Title: Supervisory Operations Specialist	Signature: GS Date signed: 6/13/13 Name: SSA Craig Severson Title: Chief Division Counsel
FBIHQ Division: [insert division name]	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

____ PIA is required by the E-Government Act.

____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ___ Yes. _X_ No: No PIA is required.

_X_ PIA is not required for the following reason(s):
- ___ System does not collect, maintain, or disseminate PII.
- ___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
- _X_ Information in the system relates to internal government operations.
- ___ System has been previously assessed under an evaluation similar to a PIA.
- ___ No significant privacy issues (or privacy issues are unchanged).
- ___ Other (describe): [redacted] b7E

Applicable SORN(s): FBI Central Records System, DOJ/FBI-002, 63 Fed. Reg. 8671 (Feb. 20, 1998), as amended by 66 Fed. Reg. 17200 (Mar. 29, 2001) and 66 Fed. Reg. 29994 (June 4, 2001).

Notify FBI RMD/RIDS per MIOG 190.2.3? _X_ No ___Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? _X_ No ___Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? ___No ___Yes (indicate forms affected):

N/A

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

			b6 b7C
[redacted] Unit Chief Privacy and Civil Liberties Unit	Signature: Date Signed:	[redacted] 7/3/12	
[redacted] Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed:	[redacted] 7/5/12	

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

The National Archives and Records Administration (NARA) Military Records Center (MRC), located in St. Louis, Missouri, houses military personnel records of individuals who formerly served in the four major branches of the Armed Forces. The St. Louis Division (SL) therefore covers a large number of leads received each year from FBIHQ, field offices, and CJIS seeking to verify the military service information of several categories of individuals, such as persons of investigative interest, applicants for federal employment, and persons seeking to purchase a firearm.

In order to more efficiently cover military service leads, several SL Investigative Operations Analysts (IOAs) [redacted] Upon receiving a lead, these IOA's query NARA databases to identify relevant military records and to electronically request retrieval of the corresponding service personnel folders by NARA personnel. The IOAs review the folders after retrieval and prepare a response to the lead, typically in the form of an EC or report, which may include copies of relevant documents, such as a court martial judgment or dishonorable discharge. The response is uploaded into the Automated Case Support System (ACS) and the original personnel folder is returned to NARA personnel. b7E

[redacted]

[redacted]

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

_____ NO

__X__ YES **[If yes, please continue.]**

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

__X__ The information directly identifies specific individuals.

_____ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

__X__ The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

___ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly.

4. Does the system/project pertain only to government employees, contractors, or consultants?

__X__ NO _____ YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ NO. **[If no, skip to question 7.]**

__X__ YES **[If yes, proceed to the next question.]**

6. Does the system/project collect any information directly from the person who is the subject of the information?

__X__ NO **[If no, proceed to question 7.]**

_____ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ NO

_____ YES **[If yes, proceed to question 7.]**

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

_____ YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

_____ NO __X__ YES **If yes, check all that apply**:

__X__ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. **Describe:**

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

_____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

8. Is the system operated by a contractor

__X__ No.

____Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

_____ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

b7E

_____ YES **If yes, please indicate the following, if known:**

Provide date of last C&A certification/re-certification:

Confidentiality:__Low__Moderate __High __Undefined

Integrity: __Low __Moderate __High __Undefined

Availability: __Low __Moderate __High __Undefined

_____ Not applicable – this system is only paper-based.

10. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

__X__ NO

_____ YES **If yes, please describe the data mining function:**

11. Is this a national security system (as determined by the SecD)?

__X__ NO _____ YES

12. Status of System/ Project:

_____ This is a new system/ project in development. **[If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]**

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? | | b7E

2. Has the system/project undergone any significant changes since April 17, 2003?

__X__ NO [If no, proceed to next question (II.3).]

_____ YES If yes, indicate which of the following changes were involved **(mark all changes that apply, and provide brief explanation for each marked change)**:

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other **[Provide brief explanation]:**

3. Does a PIA for this system/project already exist?

__X__ NO _____ YES

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

___ NO ___YES

[The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

(OGC/PCLU (Rev. 07/06/2010)

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

(Equivalent to the DOJ Initial Privacy Assessment (IPA))

NAME OF SYSTEM / PROJECT: Strategy Management Tool (SMT)

BIKR FBI Unique Asset ID: 2010-010-01-P304-104-3218

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: Strategy Management Office (SMO) Division: Director's Office (DO) Phone: [redacted] Room Number: HQ Rm 6288	**FBI OGC/PCLU POC** Name: [redacted] Phone: [redacted] Room Number: 7350

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS [complete as necessary consonant with Division policy]

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Resource Planning Office (RPO)	Signature: [redacted] Date signed: 10/22/10 Name: [redacted] Title: SMO Unit Chief	Signature: [redacted] Date signed: 10/22/10 Name: [redacted] Title: Division Privacy Officer
FBIHQ Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350). (The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

Upon final FBI approval, FBI OGC/PCLU will distribute as follows:

1 - Signed original to file 190-HQ-C1321794 (fwd to JEH 1B204)

Copies (recipients please print/reproduce as needed for Program/Division file(s)):

1- DOJ Office of Privacy and Civil Liberties (via e-mail to privacy@usdoj.gov; 1 - OGC\PCLU intranet if classified, via hand delivery to 1331 Penn. Ave. NW, Suite 940, 20530)
2- FBI OCIO / OIPP [redacted]
1- FBI SecD/AU (UC [redacted]
1- RMD/RMAU [redacted]
1- Program Division POC
1- Division Privacy Officer

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS: [This section will be completed by the FBI PCLU/PCLO following PTA submission. The PTA drafter should skip to the next page and continue.]

_____ PIA is required by the E-Government Act.

_____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ____ Yes. ____ No (indicate reason):

_X_ PIA is not required for the following reason(s):
- ___ System does not collect, maintain, or disseminate PII.
- ___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
- _X_ Information in the system relates to internal government operations.
- ___ System has been previously assessed under an evaluation similar to a PIA.
- _X_ No significant privacy issues (or privacy issues are unchanged).
- ___ Other (describe):

Applicable SORN(s): N/A

Notify FBI RMD/RIDS per MIOG 190.2.3? ___No ___Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? _X_No ___Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? _X_No ___Yes (indicate forms affected):

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

[redacted] Acting Deputy General Counsel Acting FBI Privacy and Civil Liberties Officer	Signature: Date Signed:	[redacted]	10/2/12

b6
b7C

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. **Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.**

The purpose of the Strategy Management Tool (SMT) project, owned by the Director's Office (DO)/Resource Planning Office (RPO), is to develop a technical solution to support the management of the FBI's Strategy Management System (SMS).

SMS is a strategic planning process currently being implemented throughout the FBI. Priorities are developed at the Enterprise, Branch, and Division levels and then these entities measure, track, and review performance against achieving those priorities on a quarterly basis. This is achieved through the Balanced Scorecard methodology, which includes conduct of regular strategy review meetings and the compilation of data reports that are used to facilitate the best allocation of resources for resolving critical performance issues.

The SMT project will provide the FBI with an enterprise-standard information tool to standardize this process, and allow users/divisions/branches to manage their respective SMS programs through a one-stop shop for all strategy-related items. By creating an enterprise standard information tool, the SMT project will allow the FBI to support the varying capabilities necessary for SMS success by introducing a range of processes, rules, standards, protocols, and best practices associated with the Balanced Scorecard methodology, which will facilitate common SMS usage across the FBI.

Use of SMT will be limited to only FBI personnel and authorized contract personnel. Users will access SMT through a web-based user interface, available via a FBINet log-in. No separate username or password independent of FBINet will be necessary. Access will be controlled by individual division/branch coordinators who can grant read-write or read-only access to approved personnel, as appropriate. Any revisions by a user to information contained within the SMT will be reflected in a change log. That log is visible to all division/branch coordinators and SMS objective facilitators.

Division/branch coordinators will also determine whether other divisions or branches may be granted access to their respective SMT pages. Other than those specifically authorized by the coordinators, only the Director, select Director's Office staff, and SMO staff (for management purposes) will have access to all information contained in the various division pages.

Information contained within the SMT will relate to mission scope and primarily consist of quantitative data measures, although some qualitative information is possible. It is not expected that SMT content will include any personally identifiable information other than the name of the individual posting information within SMT and his/her business contact information, nor is it expected that any specific reference will be made to FBI case information or investigative matters. To the extent sensitive or otherwise classified information is included, division coordinators will be able to classify and restrict access to the information, either in whole or in part.

SMT will reside on the Application Server Environment (ASE), and will not connect to any other FBI systems.

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

____ NO [If no, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval. Unless you are otherwise advised, no PIA is required.]

__X__ YES **[If yes, please continue.]** The system collects and identifies on each SMT page which FBI employees or authorized contract personnel have added or edited information from that page.

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

__X__ The information directly identifies specific individuals.

_____ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

_____ The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

____ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly. [If you checked this item, STOP here after providing the requested description.]

4. Does the system/project pertain only to government employees, contractors, or consultants?

_____ NO __X__ YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

__X__ NO. **[If no, skip to question 7.]**

_____ YES. **[If yes, proceed to the next question.]**

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____ NO **[If no, proceed to question 7.]**

_____ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ NO

_____ YES **[If yes, proceed to question 7.]**

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

_____ YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

__X__ NO _____ YES **If yes, check all that apply**:

_____ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. **Describe:**

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

_____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

8. Is the system operated by a contractor?

_X_ No.

____Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

__X__ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

A system security plan (SSP) for the SMT was prepared as an addendum to the Application Server Environment (ASE) and thus did not require a separate C&A to be conducted.

____ YES **If yes, please indicate the following, if known:**

Provide date of last C&A certification/re-certification:

Confidentiality: __Low __Moderate __High __Undefined

Integrity: __Low __Moderate __High __Undefined

Availability: __Low __Moderate __High __Undefined

_____ Not applicable – this system is only paper-based.

10. Is this system/project the subject of an OMB-300 budget submission?

__X__ NO

_____ YES **If yes, please provide the date and name or title of the OMB submission:**

11. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

__X__ NO

_____ YES **If yes, please describe the data mining function:**

12. Is this a national security system (as determined by the SecD)?

__X__ NO _____ YES

13. Status of System/ Project:

__X__ This is a new system/ project in development. **[If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]**

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO [If no, proceed to next question (II.3).]

_____ YES If yes, indicate which of the following changes were involved **(mark all changes that apply, and provide brief explanation for each marked change)**:

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed.

(For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other **[Provide brief explanation]:**

3. Does a PIA for this system/project already exist?

_____ NO _____ YES

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

___ NO ___YES

[The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1272295-0

Total Deleted Page(s) = 1
Page 4 ~ b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

(OGC/PCLU (Rev. 04/01/2011)

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Telecommunications Data Collection Center (TDCC) Network

BIKR FBI Unique Asset ID: APP0000247

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: IA [redacted] Program Office: Telephonic Communications Analysis Unit (TCAU) Division: Counterterrorism Phone: [redacted] Room Number: 4512	**FBI OGC/PCLU POC** Name: AGC [redacted] Phone [redacted] Room Number: 7350

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: **Counterterrorism**	Signature: [redacted] Date signed: 3/31/2013 Name: SSA [redacted] Title: Unit Chief, TCAU	Signature: [redacted] Date signed: 3.27.13 Name: Supervisory MPA [redacted] Title: Unit Chief, CTD Executive Staff
FBIHQ Division:	Signature: Date signed: Name: Title:	

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

____ PIA is required by the E-Government Act.

____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ___ Yes. ___ No (indicate reason):

__X__ PIA is not required for the following reason(s):
- ___ System does not collect, maintain, or disseminate PII.
- ___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
- ___ Information in the system relates to internal government operations.
- ___ System has been previously assessed under an evaluation similar to a PIA.
- __X__ No significant privacy issues (or privacy issues are unchanged).
- __X__ Other (describe): [redacted] b7E

[redacted]

Applicable SORN(s): DOJ-002, *DOJ Computer Systems Activity and Access Records*, 64 Fed. Reg. 73585 (Dec. 30, 1999);

Notify FBI RMD/RIDS per MIOG 190.2.3? __X__ No ___Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? __X__ No ___Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? __X__ No ___Yes (indicate forms affected):

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

[redacted] b7E

[redacted] Acting Unit Chief, Privacy and Civil Liberties Unit	Signature: [redacted] b6 b7C Date Signed: 9/19/2012
[redacted] Acting Deputy General Counsel and FBI Privacy and Civil Liberties Officer	Signature: [redacted] Date Signed: 9-19-12

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

1. Type of information in the system:

The Counterterrorism Division's Telephonic Communications Analysis Unit (TCAU) was created in 2002 to disseminate high quality intelligence based on analysis of telephone calling patterns.[1] [redacted] b7E

[redacted]

[redacted]

[redacted]

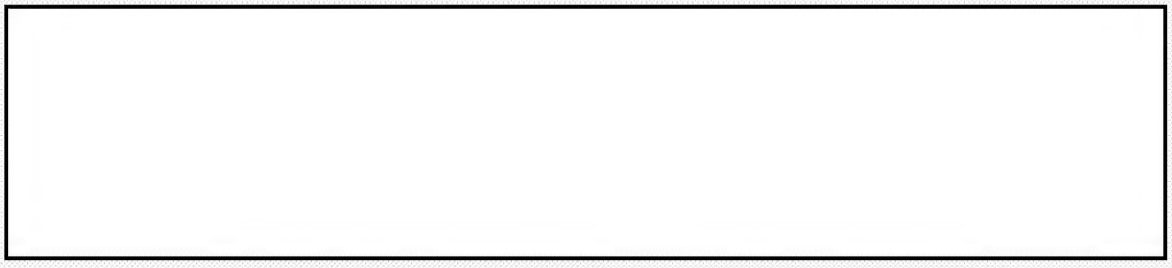
Use by TCAU Personnel

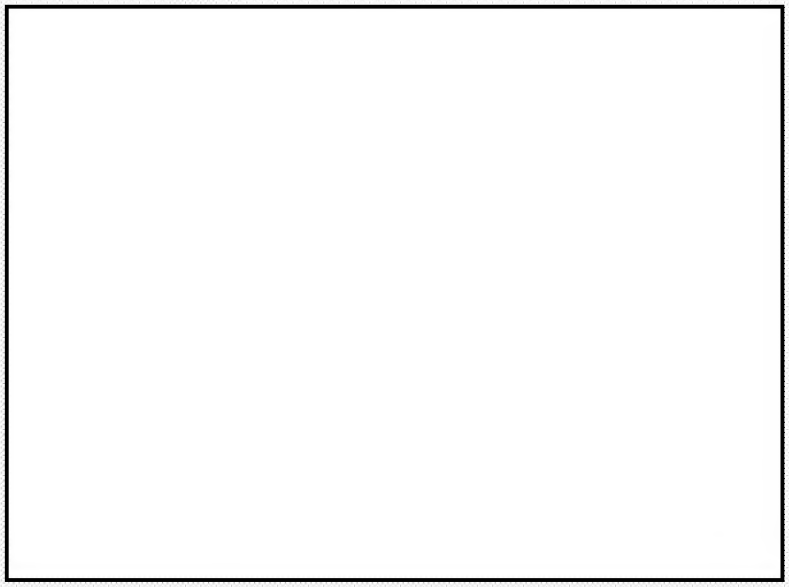
[redacted]

[1] The TCAU was known as the Communications Analysis Unit (CAU) from 2002 through September, 2012.

[redacted]

b7E





2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

_____NO [If no, STOP. The PIA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval. Unless you are otherwise advised, no PIA is required.]

__X__YES **[If yes, please continue.]**

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

_____ The information directly identifies specific individuals.

__X__ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

__X__ The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

__ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly. **[If you checked this item, STOP here after providing the requested description.]**

4. Does the system/project pertain only to government employees, contractors, or consultants?

_____ NO ___X___ YES

	b7E

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

___X___ NO. **[If no, skip to question 7.]**

_____ YES. **[If yes, proceed to the next question.]**

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____ NO [If no, proceed to question 7.]

_____ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ NO

_____ YES **[If yes, proceed to question 7.]**

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

_____ YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

__X__ NO _____ YES **If yes, check all that apply:**

_____ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. **Describe:**

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

_____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

8. Is the system operated by a contractor?

__X__ No. [redacted] b7E

____Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

_____ NO If no, indicate reason. If C&A is pending, provide anticipated completion date:

__X__ YES If yes, please indicate the following, if known:

Provide date of last C&A certification/re-certification:

The TDCC received Authority to Operate (ATO) on [redacted] an extension of its ATO is awaiting approval. b7E

Confidentiality: _X_ Low __Moderate __High __Undefined

Integrity: _X_ Low __Moderate __High __Undefined

Availability: _X_ Low __Moderate __High __Undefined

_____ Not applicable – this system is only paper-based.

10. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

_X_ NO

_____ YES **If yes, please describe the data mining function:**

11. Is this a national security system (as determined by the SecD)?

_X_ NO _____ YES

12. Status of System/ Project:

_____ This is a new system/ project in development. **[If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]**

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? January, 2004

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO [If no, proceed to next question (II.3).]

_X_ YES If yes, indicate which of the following changes were involved **(mark all changes that apply, and provide brief explanation for each marked change)**:

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

__X__ Other: [redacted] b7E

3. Does a PIA for this system/project already exist?

__X__ NO _____ YES

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

___ NO ___ YES

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [redacted] b7E

BIKR FBI Unique Asset ID: Pending

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: TSC IT Division: TSC Phone: [redacted] Room Number: TSC	**FBI OGC/PCLU POC** Name: [redacted] b6 Phone: [redacted] b7C Room Number: TSC

FBI DIVISION INTERMEDIATE APPROVALS [complete as necessary consonant with Division policy]

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: TSC IT	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:
FBIHQ Division: TSC IT	Signature: [redacted] Date signed: Name: [redacted] Title: IT Branch Chief	Signature: [redacted] Date signed: Name: [redacted] Title: TSC Privacy Officer

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

_____ PIA is required by the E-Government Act.

_____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ____ Yes. ____ No (indicate reason):

__X___ PIA is not required for the following reason(s):
- __X_ System does not collect, maintain, or disseminate PII.
- ____ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
- ____ Information in the system relates to internal government operations.
- ____ System has been previously assessed under an evaluation similar to a PIA.
- ____ No significant privacy issues (or privacy issues are unchanged).
- ____ Other (describe):

Applicable SORN(s): _N/A_____

Notify FBI RMD/RIDS per MIOG 190.2.3? _X__No ____Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? _X__No ____Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? _X__No ____Yes (indicate forms affected):

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

Elizabeth Withnell, Acting Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 9/20/12

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

[redacted] tests new features and/or modifications to existing [redacted] before implementation. The purpose of the [redacted] is to implement a testing process for determining whether requirements for systems or components are complete and correct, the software development phase fulfills the requirements or conditions imposed by the previous phase, and to insure that the final systems or components comply with specified requirements. The goal of the testing process is to detect any software development defects so that they may be corrected prior to full implementation. b7E

[redacted] provides testers the ability to run structured and ad hoc test scenarios for new functions on existing [redacted] does not contain personally identifiable information. To run tests, [redacted] uses data specifically developed by the production team. The data is created through a complex process of skewing data from [redacted] in another IT environment to create anonymized test data that does not relate to or link to individuals in any way.

Testing diagnostics are stored in the [redacted] for new functions and regression testing (see below for a description of types of testing). [redacted] is a web-based test management software that offers quality assurance for requirement management, test management, and business process testing for IT and application environments. Application issues detected in testing are reported back to the developers as [redacted] Actual test data is not stored in the [redacted] The development staff is responsible for diagnosing, prioritizing, and correcting defects and re-submitting updated code to [redacted] for re-verification.

[redacted] allows testers to run various forms of testing as follows:

New Functionality Test: All new functions are verified manually. Manual verification incorporates a human tester to run and verify the results, and requires a pre-production IT system to host the application being tested in a controlled non-development environment. The test scenarios are based on functional documentation and supporting user or system requirements defined by the business objective. During this test phase, testers take into account what the system is required to do, and how the system have been designed to meet the requirement. In other words, the test mimics functions that the system will need to perform once operational.

Regression Test: Regression tests are run to ensure existing capabilities remain supported unless they were deliberately dropped or modified as part of the new release.

Regression tests will be covered as part of end-to-end testing of new functionality and in targeted regression tests of high impact areas such as data exports.

Benchmark Test: Benchmark tests are run to ensure previous release user-focused benchmarks are met or exceeded by the current release. [redacted] user-focused benchmarks are verified manually and repeated for each release of [redacted] b7E

Cross Agency Integration Test: Cross agency tests are run to ensure the [redacted] transactional imports, exports, and reconciliation processes are not impacted by the new release and remain operational per design. The benchmark for this level of testing is to ensure that user functions, such as log-ins, saves, or searches, perform the same or better than the previous release. [redacted] currently maintains test connections with [redacted] These agencies receive test data from the [redacted] As previously stated, test data is only used for testing purposes.

The testing process begins when [redacted] receives an official build of the software once it has passed [redacted] as defined by the project schedule.

Across the [redacted] test phase (which may include several builds), the following processes occur in this order:

1. High priority tests are run; these verify the exports and functionality added or changed for the build and, if considered successful, then
2. Medium priority are run; these verify continuity of unchanged functionality and benchmark user-facing functions and, if considered successful, then
3. Low priority tests are run; these include free form, end to end tests as a final check that all documented capabilities function and are ready for production.

[redacted] testers work with the development team to diagnose and resolve identified issues throughout testing. [redacted] may request a new build when a major issue is detected or when a large number of moderate issues have been fixed and are waiting to be re-tested. [redacted]

[redacted] receives test data from [redacted] for functionality testing to ensure that new software implementation functions within [redacted] requirements. [redacted] requires users to input different login and password credentials from those used for access to [redacted] for access to [redacted] test data. This allows [redacted] to manage user accounts and facilitates user activity auditing to identify inappropriate or unauthorized use.

Prior to the testing of any new function, a Privacy Threshold Analysis (PTA) of the system is performed consistent with FBI policy to ensure that the newly anticipated functions of the system meet the appropriate legal and policy requirements.

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

__X__ NO **[If no, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval. Unless you are otherwise advised, no PIA is required.]**

_____ YES **[If yes, please continue.]**

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

_____ The information directly identifies specific individuals.

_____ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

_____ The information can b e used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

____ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly. **[If you checked this item, STOP here after providing the requested description.]**

4. Does the system/project pertain only to government employees, contractors, or consultants?

_____ NO _____ YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ NO. **[If no, skip to question 7.]**

_____ YES. **[If yes, proceed to the next question.]**

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____ NO **[If no, proceed to question 7.]**

_____ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ NO

_____ YES **[If yes, proceed to question 7.]**

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

_____ YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

_____ NO _____ YES **If yes, check all that apply:**

_____ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. **Describe:**

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

_____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

8. Is the system operated by a contractor?

_____No.

_____Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Aequisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

_____ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

_____ YES **If yes, please indicate the following, if known:**

Provide date of last C&A certification/re-certification: November 3, 2010

Confidentiality:__Basic__Moderate __High __Undefined

Integrity: __Basic __Moderate __High __Undefined

Availability: __Basic __Moderate __High __Undefined

_____ Not applicable – this system is only paper-based.

10. Is this system/project the subject of an OMB-300 budget submission?

_____ NO

_____ YES **If yes, please provide the date and name or title of the OMB submission:**

11. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

_____ NO

_____ YES **If yes, please describe the data mining function:**

12. Is this a national security system (as determined by the SecD)?

_____ NO _____ YES

13. Status of System/ Project:

_____ This is a new system/ project in development. **[If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]**

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? September 2004

2. Has the system/project undergone any significant changes since April 17, 2003?

__X__ NO [If no, proceed to next question (II.3).]

_____ YES If yes, indicate which of the following changes were involved **(mark all changes that apply, and provide brief explanation for each marked change)**:

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other **[Provide brief explanation]:**

3. Does a PIA for this system/project already exist?

___X___ NO _____ YES

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

___ NO ___ YES

[The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

(OGC/PCLU (Rev. 08/16/2010)

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Terrorist Screening Center One Way Transfer Syatem

BIKR FBI Unique Asset ID: _____

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: Terrorist Screening Center (TSC) One Way Transfer System (OWTS) Program Office: TSC Office of the Chief Information Officer (OCIO) Division: TSC Phone: [redacted] Room Number: Office 504	**FBI OGC/PCLU POC** Name: [redacted] Phone: [redacted] Room Number: 7350

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS [complete as necessary consonant with Division policy]

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: [insert division name]	Signature: [redacted] Date signed: Name: Margaret Lonergan Title: TSC CIO	Signature: [redacted] Date signed: 5/15/11 Name: [redacted] Title: Privacy Officer
FBIHQ Division: [insert division name]	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS: [This section will be completed by the FBI PCLU/PCLO following PTA submission. The PTA drafter should skip to the next page and continue.]

_____ PIA is required by the E-Government Act.

_____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ____ Yes. ____ No (indicate reason):

_X_ PIA is not required for the following reason(s):
__ System does not collect, maintain, or disseminate PII.
____ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
____ Information in the system relates to internal government operations.
____ System has been previously assessed under an evaluation similar to a PIA.
_X_ No significant privacy issues (or privacy issues are unchanged). The system amounts to infrastructure to transport information from one domain to another. The only PII that is retrievable from the system is the log-on and password information of system users.
___ Other (describe):

Applicable SORN(s): ___User information is covered by the DOJ SORN 002, Computer Systems Activity and Access Records)_____

Notify FBI RMD/RIDS per MIOG 190.2.3? _X___No ____Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? ___No ___Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? ___No ___Yes (indicate forms affected):

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 6/9/11

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

The Terrorist Screening Center's (TSC's) mission is to "[t]o consolidate and coordinate the U.S. government's approach to terrorism screening and facilitate the sharing of terrorism information that protects the Nation and our foreign partners while safeguarding civil liberties." This requires mission-critical systems to be operated at both the Unclassified and Classified security classifications. The primary purpose of the One Way Transfer System (OWTS) is to securely transport, as necessary, any data relevant to the TSC's mission from the Unclassified security classification level domain to a Classified security classification level domain. The OWTS operates only within the TSC; it does not move information from within the TSC to domains operating outside of the TSC.

The OWTS is strictly a data transport mechanism; it does not alter or transform the migrated data in any form, either systematically or via manual interaction(s). The transported data is only resident in the OWTS until the point that it has been successfully migrated to its destination, which typically occurs in under a minute but can take longer for particularly large files. As the OWTS is simply a data transport mechanism, there is very limited user access (as there is no front-end application by which users can view, edit, modify, or alter the system's data). The only users who have access to the OWTS are system administrators who are responsible to maintain and/or troubleshoot the system. Users log-in and password information is resident on the system, but this is the only personally identifiable information that is accessible.

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

__X__ NO **[If no, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval. Unless you are otherwise advised, no PIA is required.]** The only exception to this is the user log-in information.

_____ YES **[If yes, please continue.]**

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

_____ The information directly identifies specific individuals.

_____ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

_____ The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

___ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly. **[If you checked this item, STOP here after providing the requested description.]**

4. Does the system/project pertain only to government employees, contractors, or consultants?

_____ NO _____ YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ NO. **[If no, skip to question 7.]**

_____ YES. **[If yes, proceed to the next question.]**

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____ NO **[If no, proceed to question 7.]**

_____ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ NO

_____ YES **[If yes, proceed to question 7.]**

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

_____ YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

_____ NO _____ YES **If yes, check all that apply:**

_____ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. **Describe:**

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

_____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

8. Is the system operated by a contractor?

_____No.

_____Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

_____ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

_____ YES **If yes, please indicate the following, if known:**

Provide date of last C&A certification/re-certification:

Confidentiality: __Low __Moderate __High __Undefined

Integrity: __Low __Moderate __High __Undefined

Availability: __Low __Moderate __High __Undefined

_____ Not applicable – this system is only paper-based.

10. Is this system/project the subject of an OMB-300 budget submission?

_____ NO

_____ YES **If yes, please provide the date and name or title of the OMB submission:**

11. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

_____ NO

_____ YES **If yes, please describe the data mining function:**

12. Is this a national security system (as determined by the SecD)?

_____ NO _____ YES

13. Status of System/ Project:

_____ This is a new system/ project in development. **[If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]**

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO [If no, proceed to next question (II.3).]

_____ YES If yes, indicate which of the following changes were involved **(mark all changes that apply, and provide brief explanation for each marked change)**:

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed.

(For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other **[Provide brief explanation]:**

3. Does a PIA for this system/project already exist?

_____ NO _____ YES

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

____ NO ____ YES

[The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

Form Rev. 9/9/08

CHECKLIST FOR PRIVACY COMPLIANCE FOR FBI ROUTINE DATABASES
(including comparable applications)

NAME OF SYSTEM / PROJECT: [redacted] b7E

FBI Unique Asset ID: APP-0000004

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [redacted] Program Office: ITB Division: ITSD Phone: [redacted] Room Number: 8977	FBI OGC/PCLU POC Name: [redacted] [redacted] Phone: [redacted] Room Number: 9320

b6
b7C

This checklist is based on the FBI Privacy Impact Assessment (PIA) for FBI Routine Databases of 4/7/08 as approved 8/29/08 (190-HQ-C1321794 Serial 432, 9/8/08). In accordance with the PIA, this checklist may be used in lieu of any additional PIA (or PTA), so long as every one of the twelve blocks below can be checked. This checklist should be completed by the database manager (or other appropriate official/ as determined by the division) and approved by the Division Privacy Officer.

A. Provide date checklist prepared: 6/4/2010

B. Provide a general description of the system or project that includes: name of the system/project, including associated acronyms; structure of the system/project, purpose; nature of the information in the system and how it will be used; who will have access to the information in the system and the manner of transmission to all users.

[redacted] b7E

b7E

C. Complete checklist (all must be checked as being accurate for this database/application):

__X__ 1. Information in the system identifies individuals, either directly or indirectly. An individual can be identified indirectly through a combination of descriptors such as gender, race, birth data, geographic indicator, license number, or license plate number.[1]

__X__ 2. The system derives information from FBI records covered by existing Privacy Act system of records notices (http://foia.fbi.gov/rec_sys.htm) regardless of format in which those records are maintained and/or from information that is publicly available at no cost. (If information comes from FBI records that are not covered by existing systems of records notices, contact the PCLU.)

__X__ 3. Neither commercial data nor paid subscription service data is included in the database unless that information is derived from existing FBI records.

__X__ 4. The system can be accessed only by members of a particular office, unit, squad or other similar FBI entity and sharing of information is based strictly on an operational need to know.

__X__ 5. The system is not used for purposes of pattern-based data mining.

__X__ 6. Initial and continued access to the system is subject to permission controls enforced by FBI supervisory personnel, including the use of access passwords.

__X__ 7. Access to the system can be audited.

__X__ 8. The system is part of an established platform on which a Security Certification and Accreditation has been performed.

__X__ 9. The system was developed after April 17, 2003.[2]

---

[1] Systems that do not contain any personally identifiable information need not complete this checklist.

[2] Systems developed before April 17, 2003, and not modified since then are not required to conduct a PIA until a modification occurs that would change the privacy risks to information in the system.

X 10. If the system maintains information about U.S. citizens or legal permanent residents, it is covered by a published Privacy Act System of Records Notice.

X 11. Records retention issues have been discussed with the Records Management Division.

X 12. Any personally identifiable information placed on a mobile device or on media that is transported outside FBI facilities must comply with the FBI policy on encryption and must be password protected.

D. If a database contains information that may be considered sensitive/controversial or is maintained as part of a larger FBI program, the database administrator or program manager (or division privacy officer) must consult with the FBI's Office of the General Counsel, Privacy and Civil Liberties Unit about the potential need to assess the privacy risks in a separate PIA.

E. File Notes (summarize any additional information that may be warranted for record purposes, e.g., coordination with OGC, etc.):

APPROVING OFFICIALS

Program Manager (or other appropriate official as division determines)	Division Privacy Officer
Signature: [redacted] Date signed: 6-9-10 Name: Name: [redacted] Title: Unit Chief, USOU	Signature: [redacted] Date signed: 6/24/10 Name: [redacted] Title: Unit Chief, SPU

b6
b7C

DISTRIBUTION:
- File signed original (or copies) in one or more official division/program files for documentation, inspection, records, and other oversight purposes.
- Forward copy to the FBI Privacy and Civil Liberties Unit (PCLU) (JEH 7338).

Privacy Impact Assessment for FBI Routine Databases

The Federal Bureau of Investigation manages its information resources in an electronic environment that facilitates the collection of a wide variety of data. The current electronic environment, however, is not always flexible enough to meet the ever-increasing demands of the Bureau for situational awareness, strategic planning, and reporting. Consequently, a majority of Bureau units have or are considering developing routine databases,[3] using Microsoft Access[4] or other standard applications, to repackage Bureau information into a format that more closely meets operational requirements. These routine databases combine information already collected by the FBI and maintained in its case management system (the Automated Case Management system or ACS) or its administrative records, but permit a combination of data in ways that may reveal additional useful information about events and the individuals associated with them.

Routine databases created in the FBI share common characteristics. They are created using approved applications and are maintained primarily on local servers that are connected to the FBI's internal computer network. Supervisors in an office, squad or program typically function as the database administrator and assign access privileges to employees, contractors or task force members based on need to know and role. They can also perform oversight of database use in order to detect anomalies. Routine databases are password protected to further limit access. Information in these databases, which may take the form of spreadsheets, word processing documents, as well as the more typical database applications, is derived from information already collected by the FBI for mission-related purposes, for which Privacy Act system of records notices have been published as necessary, or is information available to the public at no cost. To the extent that data is derived from ACS, permission to extract the data is controlled by the FBI's Information Technology Operations Division and is subject to control by the FBI division owner of the originating information.

When a system uses technology to manipulate existing data about individuals in a way that the data is no longer functionally obscure but, instead, may be readily retrievable, a Privacy Impact Assessment (PIA) is required by both FBI policy (see, e.g.,

---

[3] For purposes of this PIA, the term "routine database" is used to signify those databases, spreadsheets or even word processing programs that are employed to manipulate existing FBI data, but that do not rise to the level of a major information system. The routine databases at issue are all covered by the certification and accreditation of an established FBI Federal Information Security Management Act (FISMA) system.

[4] Microsoft Access permits the creation of a relational database management system that allows users to organize, query, manipulate, link and view data from multiple sources and to use the resultant information for operational purposes as well for statistical reporting requirements. In the case of the Microsoft Access databases covered by this Privacy Impact Assessment, ACS will provide the source for information. Reference to Microsoft Access implies no endorsement of this particular product, but is simply a reflection of the fact that this software, among others, is employed in the FBI.

Privacy Impact Assessments and Privacy Threshold Analyses, Updated Guidance, 66F-HQ-1201415 (Dec. 21, 2006)), DOJ Order 3011.1A, and by Section 208 of the E-Government Act and the implementing guidance published by the Office of Management and Budget. Experience has demonstrated, however, that routine databases meeting certain criteria all contain similar privacy risks and mitigate those risks in similar ways. Therefore, individual PIAs for such databases tend to be repetitive in nature.

This PIA is intended to cover all routine databases that meet the system description contained herein. If all criteria described below are met, then this PIA satisfies the FBI and E-Government Act privacy assessment requirements. To verify that this is the case, a checklist has been developed (attached as an appendix) that must be completed by the database owner and provided for review and approval, along with a description of the compliant database, to both the pertinent Division Management and its Privacy Officer as well as to the FBI Privacy and Civil Liberties Officer. Copies of approved checklists should be maintained by Division Privacy Officers and available for inspection upon request.

Section 1.0
The System and the Information Collected and Stored within the System.

1.1 What information is to be collected?

A routine database will extract and store personally identifiable data from existing FBI records or from records that are available to the public at minimal cost, such as Internet search engines or the news media.[5] The data may be derived from ACS, the Bureau's main case management system.[6] It may also consist of administrative information that the FBI otherwise maintains, such as payroll or personnel data. The databases may be maintained by an FBI Headquarters division or office or locally by a field division. If a database contains information that may be considered sensitive or controversial or is maintained as part of a larger FBI program, the database administrator or program manager must consult with the FBI's Office of the General Counsel, Privacy and Civil Liberties Unit about the need to assess the privacy risks in a separate PIA.

1.2 From whom is the information collected?

The information is provided by individuals and/or is collected by FBI personnel. Case-related information is derived from interviews, investigations or other activities

---

[5] Paid subscriptions to databases maintained by commercial data brokers in general do not meet the requirement for "at minimal cost."

[6] As the FBI converts its case management system from ACS to Sentinel, the need for routine databases may diminish. This PIA, however, is intended to cover any such databases that are created based on information in the FBI's primary case management system or other existing files.

performed pursuant to the FBI's mission. Administrative information is collected from employees, contractors or others who perform work for the FBI. Routine databases do not include information from commercial databases unless that information was previously incorporated into the other FBI records from which information in the routine database is derived. Information in the databases, however, may be obtained from sources that any member of the public could access at minimal cost.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

2.1 Why is the information being collected?

The information has already been collected in support of the work of the FBI unit that will use the database or is obtainable from public sources, but it is being reconfigured into a functional format so that it can be manipulated in order to meet reporting requirements, to improve situational awareness, to facilitate strategic planning and to make associations within the data, if any, more apparent.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

The general authority for the FBI to investigate crimes, including terrorism, and to acquire, collect, classify and preserve records pertaining to those investigations can be found in 28 U.S.C. §§ 533 and 534. The FBI also has jurisdiction over specific crimes as a result of more narrowly focused legislative enactments and has intelligence responsibilities pursuant to the Patriot Act and other statutes. Administrative information is collected pursuant to the general government authority for this purpose.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

The information in the routine databases covered by this assessment duplicates information that the FBI has legally collected and maintains in another FBI system(s) or is information that is publicly available. There is a privacy risk from the recombination of information into a separate database, because connections among the data that might have been obscure could become more apparent. One of the reasons for using available application software, however, is precisely to make these connections more transparent. This privacy risk is mitigated by the fact that access to these databases is limited to a squad, unit or office that is likely already to have access to the information that will populate a routine database, but needs the added benefit of the software tools to improve its ability to pursue law enforcement or terrorism assignments, provide analysis, conduct administrative operations and create required reports.

Section 3.0
Uses of the System and the Information.

3.1 Describe all uses of the information.

As noted in the previous section, the information will be used for tactical, strategic and reporting purposes. The recombination of information from existing FBI systems can help highlight important aspects of what is known about individual cases in ways that improve situational awareness and facilitate the appropriate use of resources. Information can be aggregated for reporting purposes and disaggregated in order to focus more clearly on significant incidents or people. Administrative information can be manipulated to produce analyses and reports.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (sometimes referred to as data mining)?

Data mining involves the use of sophisticated data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. While a by-product of the use of routine databases may be the ability to discern relationships among data that previously were not apparent, the use of these databases is not for purposes of data mining, but for improved data management. Large data sets are not being created in order to infer rules that allow for the prediction of future results -- one of the hallmarks of data mining -- and, in fact, any system that creates large data sets would require a separate privacy analysis. Smaller databases are being created from information maintained in ACS or elsewhere in order to more effectively manage and control data that will be useful for operational, strategic or administrative purposes.

3.3 How will the information collected from individuals or derived from the system, including the system itself, be checked for accuracy?

Because the FBI needs the flexibility to collect a wide variety of information for law enforcement purposes from a wide variety of sources, that information is not always accurate, complete, timely and relevant. This is primarily due to the fact that at the time of collection it is typically impossible to ascertain that the information meets these requirements. With the passage of time or when viewed in connection with other information, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The FBI, nevertheless, has a business need to maintain accurate records. Before the information that will be combined into the routine databases at issue is used for operational purposes, it is checked to ensure its integrity. Routine databases, moreover, are generally employed by squads or units that

are already familiar with the information to be included. If an anomaly occurs during data manipulation, individual users have the ability to examine the source information and other data to correct the anomaly as necessary. In this vein, the recombination of existing FBI data into a routine database may reveal that the original information requires revision or updating. Consequently, these routine databases may themselves contribute to overall information accuracy. For routine databases containing administrative data, the information can be checked for accuracy against the source files.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

The disposition of routine database records is directly managed by the Records Disposition Unit of the Records Management Division, which works with FBI system owners and NARA to develop disposition authorities for these electronic information systems.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The FBI's purpose in using routine databases is to facilitate the ability of individual offices, squads or programs to provide accurate and timely information for a variety of uses. There is an incentive to ensure that the information is correct because otherwise any resultant products, such as reports, will be inaccurate. As an enforcement and oversight mechanism, Division managers and Privacy Officers must review and approve a checklist that each program officer completes for a particular application to demonstrate compliance with the attributes required for approval. Oversight of this process will be provided through the FBI's Inspection Division working in conjunction with the Privacy and Civil Liberties Officer.

Controls on the use of information in these routine databases are applied at the user level and at the program level. Users are limited to the members of a division, squad or office who are provided access based on a defined need to know and an appropriate role requiring access to the data. Oversight is provided through the grant of access initially and through the ability to audit system use, including the ability to recommend disciplinary action for misuse. In addition, program controls are applied through supervisors who grant access to these databases and through the FBI's Inspection Division, which conducts periodic compliance reviews.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

4.1 With which internal components of the Department is the information shared?

The information will be shared within the FBI with those units that have a need for access in order to perform their mission. In some cases, the information is shared with members of task forces or detailees from other agencies, but sharing in these circumstances is considered internal and recipients are expected to comply with any internal FBI policies regarding access and use of the data.

4.2 For each recipient component or office, what information is shared and for what purpose?

The FBI unit or office that creates the database establishes the rules for access, but typically access is limited to those within the unit or office that have a need for access to perform mission-critical tasks. Sharing beyond this core group typically does not take place, but the data may be used for reporting purposes and those reports would be shared more broadly based on operational need.

4.3 How is the information transmitted or disclosed?

Transmission is primarily electronic and may be done through electronic media or over a network.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Because the information that populates routine databases is derived from data that already exists within the FBI or consists of public source material, there is a privacy risk that additional knowledge may be available from the combination of data that otherwise would not be apparent. This risk is also the benefit of using these routine applications to better understand what information an individual program has or knows. This risk is mitigated by limitations on individuals who can access the data in its combined form. Many routine databases are created for the convenience of a squad, unit, or office, and a database administrator limits access rights to those with a bona fide need to know. Passwords for access may also be employed to enhance the security and privacy of the information. In addition, any transfer of the information to mobile devices must meet the requirements of FBI policy for protecting information on mobile devices.

There is also a privacy risk that the replication of data from one database to another could result in the production of erroneous data through keystroke errors. The routine databases, however, are typically checked by supervisors to ensure data integrity and thus minimize that risk. There is a further privacy risk from the fact that the ability to audit these routine databases is not as robust as in other more sophisticated systems. But as a precondition of approval for these routine databases, the attached checklist requires the completing official to signify that there is an ability to audit access and use, so the privacy risk is reduced. If an individual user is found to be accessing the database inappropriately, disciplinary action can be taken. In addition, these databases will be subject to the FBI's periodic inspection process to ensure compliance with the requirements for database approval.

Section 5.0
External Sharing and Disclosure

5.1 With which external (non-DOJ) recipient(s) is the information shared?

No system-to-system sharing between an FBI routine database and an external recipient is contemplated. Instead, disclosures of discrete pieces of information may be made, as appropriate, to other federal, state, local, tribal or foreign law enforcement entities, Congress or the public in the same manner as such disclosures are made of information from the underlying systems. For example, if information from a routine database reveals criminal activity in a particular location, the FBI office maintaining the database may share that information with appropriate state or local law enforcement. This kind of routine sharing, which is subject to rules governing need to know, restrictions on further dissemination (as appropriate) and other limitations, already regularly occurs and the creation of these routine databases will not alter this. Alternatively, the routine databases may be used to develop required reports. In many cases, if data is used in reports that will be made public, the data will be stripped of identifiers, unless there is a need for their inclusion. External reporting, for example, of personnel information that may be derived from a routine database would likely not include individual employee names unless there was a business reason for doing so.

5.2 What information is shared and for what purpose?

See previous response.

5.3 How is the information transmitted or disclosed?

If sharing occurs, it could be by any means necessary to effect the transfer of discrete pieces of information -- electronic, paper or otherwise.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

In the event information is shared externally and it includes personal identifiers, the sharing is subject to FBI corporate policy and controls regarding security and privacy that govern any disclosures of information from FBI files.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

The external sharing that is contemplated will be consistent with disclosures currently made from FBI records. If training is required to understand the FBI information, it is provided on an individual basis. Because there will be no disclosures between these routine databases and other agency systems, however, there is no need for training on use of these databases.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

As noted in the previous response, system-to-system disclosures will not be made. When disclosures are made from FBI records generally, any caveats on use of the information are associated with the data at the time of the disclosure.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The type of sharing of information from routine databases that is likely to occur is no different from the disclosures currently made from the underlying FBI records, and thus any sharing will be subject to current processes and limitations on the access to and use of FBI information. If personally identifiable information is downloaded to mobile devices for purposes of external sharing, FBI policy requires that it be adequately protected in transit through the use of passwords and encryption software. Consequently, there should be no additional privacy risk from the external sharing of the information. In many cases, moreover, information to be shared will not contain personal identifiers.

Section 6.0
Notice

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

Individuals are typically not provided a separate notice about the disposition of information collected from them in connection with a law enforcement or national security investigation. General notice is available, however, through publication of Privacy Act System of Records notices that govern information the FBI collects and maintains. The majority of information to be placed in the databases covered by this PIA would be covered by the system notice for the FBI's Central Records System, last published in the Federal Register on February 20, 1998 (63 Fed. Reg. 8671). When information is collected primarily for administrative purposes, notice is usually provided on the form used for the collection.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

In many cases, the information at issue will be obtained through the results of investigations. In most cases, there is no right to decline to provide information. In those cases where there is a right not to participate in or cooperate with an investigation, or otherwise not provide information, the individual may be afforded that opportunity. When information is collected primarily for administrative purposes, the collection itself may be voluntary and thus the individual would have the right to decline to provide it.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

If an individual has placed any enforceable restrictions on the use of information that the FBI has otherwise collected, those restrictions would follow recompilation of the information into a routine database. There is no other opportunity to consent to or restrict particular uses of the database information.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The system notice for the FBI's Central Records System, from which the majority of information will be obtained, explains that the "FBI uses its computers, when necessary, to collate, analyze, and retrieve investigative information in the most accurate and expeditious manner possible." It also states that the FBI supports complicated investigative matters by using specialized computer systems or individual microcomputers and that duplicate records and extracts of information are kept in various FBI divisions to assist in day-to-day operations. Thus, the public is on notice that the FBI combines the information it receives in ways designed to collate, analyze and retrieve information. This transparency helps to mitigate the privacy risk that accompanies recompilation of information from one collection into another routine database where relationships among the data may become more apparent.

Section 7.0
Individual Access and Redress

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information.

Individuals are entitled to avail themselves of the procedures outlined in 28 C.F.R. Part 16 in order to seek access or redress of their own information. Although many of the FBI's files are exempt from the access and amendment requirements of the Privacy Act, the FBI has a business need for accurate records and may, in its discretion, permit individuals to supply statements disputing particular facts in FBI records.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

Information on how to submit a Freedom of Information Act/Privacy Act request to the FBI is contained on the FBI's Internet site, www.fbi.gov and in 28 C.F.R. Part 16.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

Although the FBI's law enforcement record systems are typically exempt from the access and amendment provisions of the Privacy Act, in its discretion, the FBI may accept one page statements of disagreement about facts maintained in its records. This provides a means of redress in cases where data may be inaccurate or otherwise lacking in integrity and the records are not otherwise subject to amendment or correction.

7.4 Privacy Impact Analysis. Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

As noted in the previous response, in its discretion the FBI considers requests for amendment/correction of its law enforcement records. Judicial review is also available in appropriate cases when an individual wishes to challenge action taken in reliance on information derived from FBI records from a particular database.

Section 8.0
Technical Access and Security

8.1 Which user group(s) will have access to the system?

Each office, unit or squad that uses routine databases defines its own rules for access based on operational need.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

It is possible that contractors located in particular offices, units or squads will have access to the databases covered by this PIA. In that event, however, contractors would be treated like employees and subject to the same restrictions on access and use. In addition, contracts with vendors that involve personally identifiable information contain the relevant Federal Acquisition Regulation provisions requiring Privacy Act compliance.

8.3 Does the system use "roles" to assign privileges to users of the system?

The answer depends on the rules established for each database, but generally a supervisor manages the database and users have read, write, or read and write access, depending on their office function.

8.4 What procedures are in place to determine which users may access the system and are they documented?

Because the databases are created by individual offices, units or squads, users are determined by the database creators/supervisory personnel. While written documentation may not be available in all cases, the checklist that each system supervisor must complete requires acknowledgment that access is limited only to those with an operational need to know.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The assignment of roles is subject to supervisory approval and is based on mission requirements and the individual's need for access to perform his or her duties. The databases that are created using routine software must be capable of being audited to ensure that the data is being used consistent with the purpose for which the database was created and the database must operate on a platform for which a Certification and Accreditation has been performed. In most instances, the routine databases at issue will operate on the FBI's internal computer network.

8.6 What auditing measures and technical safeguards in place to prevent misuse of data?

See previous answer.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All FBI employees, contractors and task force members are required to complete yearly information security training which contains a substantial privacy component. Additional privacy training is available on an ad hoc basis to individual FBI divisions or groups. In addition, the FBI has developed training on the use of U.S. person

information that is available Bureau-wide. Other training is provided in connection with specific programs or systems.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification and Accreditation last completed?

As noted previously, routine databases operate primarily on the FBI's computer network, which has been subjected to the C& A process. The system on which these databases operate was recertified and reaccredited in January 2008.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Routine databases, using Microsoft Access or other software applications that have been approved for use throughout the FBI, help divisions, offices and squads manage information in a manner that effectively meets mission needs. These routine databases operate primarily on the FBI's internal computer network, which meets Certification and Accreditation requirements. The information that populates these databases is derived from other FBI information systems or can be obtained by any member of the public. The recombination of data from these sources may result in new information being accessible that was previously obscure or unavailable. The privacy risk from this recombination, however, is mitigated by the fact that access to the databases is limited in each instance to those with an operational need to know and is controlled by supervisory personnel. In addition, to the extent that a clearer picture of an event or individual emerges, these databases may help increase data accuracy and integrity.

Conclusion

To increase FBI efficiency and enhance operations, the FBI employs routine database technology to manage its information resources for purposes of situational awareness, strategic planning and reporting. The privacy concerns associated with the use of these databases are mitigated and outweighed by the benefits of enhanced information knowledge that flows from the use of this technology.

Reviewing Officials

_____ (Sign Date)
Elizabeth Withnell, Unit Chief
Privacy and Civil Liberties Unit

_____ (Sign Date)
David C. Larson
FBI Privacy and Civil Liberties Officer

Approved 8.29.08 _____ (Sign Date)
Kenneth P. Mortensen
Acting Chief Privacy and Civil Liberties Officer
Department of Justice

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Web-based Automated Case Support (WACS)

BIKR FBI Unique Asset ID: APP-000003

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: System Support Section/Case Management Support Unit Division: IT Services Phone: [redacted] Room Number: 8379	**FBI OGC/PCLU POC** Name: [redacted] Phone: [redacted] Room Number: 7350

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: (Not Applicable)	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title: [redacted]
FBIHQ Division: ITSD	Signature: [redacted] Date signed: 2/28/11 Name: James E. Short, Jr. Title: Section Chief, Systems Support	Signature: [redacted] Date signed: 2-24-11 Name: [redacted] Title: Chief, Process Policy and Metrics Unit

b6
b7C

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

_____ PIA is required by the E-Government Act.

_____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ____ Yes. ____ No (indicate reason):

__x__ PIA is not required for the following reason(s):
- _x_ System does not collect, maintain, or disseminate PII.
- ___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
- ___ Information in the system relates to internal government operations.
- ___ System has been previously assessed under an evaluation similar to a PIA.
- ___ No significant privacy issues (or privacy issues are unchanged).
- ___ Other (describe):

Applicable SORN(s): _____

Notify FBI RMD/RIDS per MIOG 190.2.3? ___No ___Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? ___No ___Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? ___No ___Yes (indicate forms affected):

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

Elizabeth R. Withnell, Acting Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed:

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

The Web-based Automated Case Support (WACS)[1] application is a web-based interface that provides access to several key and commonly-used functions within the FBI's Automated Case Support (ACS) system via a standard Web browser. [redacted] b7E

WACS [redacted] is accessible to authorized FBI employees, contractors, and task force members via the FBINet enclave, which is classified at the Secret level. The system is not accessible to the general public. b7E

WACS does not store/maintain any data; rather, it simply acts as another means of accessing and interfacing with ACS. [redacted] b6 b7C

WACS runs on the FBI's mainframe. [redacted] b7E

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

__X__ NO **[If no, please stop.]**

_____ YES **[If yes, please continue.]**

3. Please indicate if any of the following characteristics apply to the information in the system about individuals. Bear in mind that log-on information may identify or be linkable to an individual. (Check all that apply.)

_____ The information directly identifies specific individuals.

_____ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

[1] WACS was previously known as Phoenix.

_____ The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

_____ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly.

4. Does the system/project pertain only to government employees, contractors, or consultants?

_____ NO _____ YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ NO **[If no, skip to question 7.]**

_____ YES **[If yes, proceed to the next question.]**

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____ NO **[If no, proceed to question 7.]**

_____ YES, however the information is not entered by the person who is the subject of the information, but rather by FBI personnel who acquire such information in the performance of their official duties.

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ NO

_____ YES **[If yes, proceed to question 7.]**

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

_____ YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

_____NO _____ YES **If yes, check all that apply:**

_____ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. **Describe:**

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

_____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

8. Is the system operated by a contractor?

_____NO

_____YES. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

_____ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

_____ YES **If yes, please indicate the following, if known:**

Provide date of last C&A certification/re-certification:

Confidentiality: __Low __Moderate __High __Undefined

Integrity: __Low __Moderate __High __Undefined

Availability: __Low __Moderate __High __Undefined

_____ Not applicable – this system is only paper-based.

10. Is this system/project the subject of an OMB-300 budget submission?

_____ NO

_____ YES **If yes, please provide the date and name or title of the OMB submission:**

11. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

_____ NO

_____ YES **If yes, please describe the data mining function:**

12. Is this a national security system (as determined by the SecD)?

_____ NO _____ YES

13. Status of System/ Project:

_____ This is a new system/project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO **[If no, proceed to next question (II.3).]**

_____ YES **[If yes, indicate which of the following changes were involved (mark all changes that apply, and provide brief explanation for each marked change):**

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other **[Provide brief explanation]:**

3. Does a PIA for this system/project already exist?

_____ NO _____ YES

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

_____ NO _____ YES

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [redacted] b7E

BIKR FBI Unique Asset ID: N/A

	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
	Name: [redacted] Program Office: Operating Systems Support Unit (OSSU) Division: ITSD Phone: [redacted] Room Number: PSC RM 117	Name: AGC [redacted] Phone: [redacted] Room Number: JEH, Rm 7350

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Infrastructure Support Section	Signature: [redacted] Date signed: 04/11/13 Name: [redacted] Title: Supervisory IT Specialist	Signature: [redacted] Date signed: 5/7/2013 Name: [redacted] Title: A/ Supervisory
FBIHQ Division: Information Technology Services Division (ITSD)	Signature: [redacted] Date signed: 4/15/13 Name: [redacted] Title: OSSU Unit Chief	Signature: Date signed: Name: Title:

b6
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

_____ PIA is required by the E-Government Act.

_____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ___ Yes. ___ No

__X__ PIA is not required for the following reason(s):
- ___ System does not collect, maintain, or disseminate PII.
- ___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
- __X__ Information in the system relates to internal government operations.
- ___ System has been previously assessed under an evaluation similar to a PIA.
- __X__ No significant privacy issues (or privacy issues are unchanged).
- ___ Other:

Applicable SORN(s): DOJ Computer Systems Activity and Access Records (DOJ-002) and The FBI Central Records System (Justice/FBI-002)

Notify FBI RMD/RIDS per MIOG 190.2.3? __X__ No ___ Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? __X__ No ___ Yes

Prepare/revise/add Privacy Act (e)(3) statements for related forms? __X__ No ___ Yes

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

[redacted] Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed: 5/8/12
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 5/16/12

b6
b7C

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

The FBI operates many [redacted] b7E

[redacted] b7E

[redacted] b7E

[redacted] The only PII maintained will be the user name as it appears within the audit log.

Only a select group of individuals have access [redacted] and they must log in [redacted] using their unique user ID and password. Based on the user's login information, the [redacted] is able to determine what access the individual should have within the system. [redacted] b7E

[redacted] There will be no general users who have direct access to the [redacted]

An audit log captures all activity within the [redacted] including the user's name, date, time, what action occurred, and what commands were run by the user. b7E

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

__X__ NO **The only PII is the user name contained within the audit log.**

____ YES

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

_____ The information directly identifies specific individuals.

_____ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

_____ The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

__/__ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly.

[If you checked this item, STOP here after providing the requested description.]

4. Does the system/project pertain only to government employees, contractors, or consultants?

_____ NO _____ YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ NO. **[If no, skip to question 7.]**

_____ YES. **[If yes, proceed to the next question.]**

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____ NO **[If no, proceed to question 7.]**

_____ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ NO

_____ YES **[If yes, proceed to question 7.]**

b. Are subjects of information from the individuals that the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

_____ YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

_____ NO _____ YES **If yes, check all that apply:**

_____ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. **Describe:**

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

_____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

8. Is the system operated by a contractor?

_____No.

_____Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

_____ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

_____ YES **If yes, please indicate the following, if known:**

Provide date of last C&A certification/re-certification:

Confidentiality: __Low __Moderate __High __Undefined

Integrity: __Low __Moderate __High __Undefined

Availability: __Low __Moderate __High __Undefined

_____ Not applicable – this system is only paper-based.

10. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

_____ NO

_____ YES **If yes, please describe the data mining function:**

11. Is this a national security system (as determined by the SecD)?

_____ NO _____ YES

12. Status of System/ Project:

_____ This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO [If no, proceed to next question (II.3).]

_____ YES If yes, indicate which of the following changes were involved **(mark all changes that apply, and provide brief explanation for each marked change):**

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other **[Provide brief explanation]:**

3. Does a PIA for this system/project already exist?

_____ NO _____ YES

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

___ NO ___YES